PART IV

(Pages 151-200)

Publication No. EP 0950968

Dated: 02-1999

(English Publication of WO 9909502 corresponding to Korean Publication No. 2000-0068758)

(Previously filed in IDS of December 5, 2007)

examine the amount of payment 11303, the card status 11304 and the total remaining value 11305 that have been modified to determine whether they match.

[1463] In the telephone card reference process, first, the service providing system examines the registered card list 5502 to determine whether the electronic telephone card has been registered. Then, the service providing system employs the user public key 5519 to examine the user digital signature in the telephone micro-check, and employs the registered card certificate to examine the card digital signature in the telephone micro-check. Further, the service providing system employs the micro-check issuing number to examine the amount of payment 11303, the card status 11304 and the total remaining value 11305 that have been modified to determine whether they match.

[1464] The telephone micro-check list address 5521 is an address in the service director information server 901 at which is stored list information for a telephone micro-check (a telephone micro-check that is uploaded to the service providing system in the telephone card reference process).

[1465] The former user information address 5522 is an address in the service director information server 901 at which is stored former user information 5523 concerning a preceding owner (user) of the electronic telephone card. When an electronic telephone card that is registered is transferred to another user, the service providing system updates the registered card list 5502 to reflect the new user information, and the old user information is managed as the former user information 5523.

[1466] The former user information 5523 consists of five types of information: a user ID 5524, a user public key 5525, a registered card certificate address 5526, a micro-check list address 5527, and a former user information address 5528. These addresses correspond respectively to the user ID 5518, the user public key 5519, the registered card certificate address 5520, the micro-check list address 5521 and the former user information address 5522, all of which are in the registered card list. In addition, when another owner preceded the present owner, the former user information address 5528 is an address of the former user information for the pertinent owner.

[1467] That is, when the electronic telephone card that is registered is transferred, the user ID 5518, the user public key 5519, the registered card certificate address 5520, the micro-check list address 5521, and the former user information address 5522 are updated, and at the former user information address 5522, the information stored in those portions before the updating is pointed to as the former user information 5523.

[1468] Since the electronic telephone card is managed in the above described manner, the usage condition of the electronic telephone card can be precisely understood even when it is transferred. Thus, even when the transfer of an electronic telephone card that is partially used is permitted, the safety of the system is not deteriorated.

[1469] A detailed explanation will now be given for the contents of messages that are exchanged by devices, and the operations performed by the individual devices during the mobile electronic commerce service processing.

[1470] First, an explanation will be given for the contents of messages that are exchanged by devices, and the operations performed by the devices during the individual processes performed for network hierarchial storage and management.

[1471] An explanation will now be given for the contents of messages that the mobile user terminal 100, the gate terminal 101, the merchant terminal 102 and the merchant terminal 103 exchange with the service providing system 110 in the remote access process. The remote access process is a process for the downloading of data from the service providing system 110 in order to access data at a remote address. This process is hereinafter called a remote access process.

[1472] In Fig. 56A is shown the remote access process performed by the mobile user terminal 100, and in Figs. 85A and 85B are shown the contents of the messages that are to be exchanged by the mobile user terminal 100 and the service providing system.

[1473] When data to be accessed is located at the remote address, the mobile user terminal 100 generates a remote access request 5600, i.e., a message requesting that the user processor in the service providing system 110 access data, and transmits it to the user processor.

[1474] As is shown in Fig. 85A, a digital signature 8504 of a user is provided for data that consists of a remote access header 8500, which is header information indicating the message is the remote access request 5600 and describing the data structure of the request; a data address 8501, which indicates a remote address; a user ID 8502; and an issued time 8503, which indicates the date when the remote access request 5600 was issued. The data are closed and are addressed to the service provider, thereby providing the remote access request 5600.

[1475] The user processor in the service providing system 110 receives the remote access request 5600, decrypts it and examines the digital signature, and generates a remote access data message 5601 and transmits it to the mobile user terminal 100.

[1476] As is shown in Fig. 85B, the digital signature of a service provider is provided for data that consist of a remote access header 8508, which is header information indicating that the message is the remote access data 5601 and describing the data structure of the remote access data; data that are requested 8509; a service provider ID 8510; and an issued time 8511, which indicates the date on which the remote access data 5601 was issued. The data are closed and addressed to the user, thereby providing the remote access data 5601.

[1477] The mobile user terminal 100 receives the remote access data 5601, decrypts it, examines the digital signature, stores it in the temporary area, and accesses the data.

[1478] Similarly, in Fig. 57A is shown the remote access process performed by the gate terminal 101 or the merchant terminal 102 or 103, and in Figs. 86A and 86B are shown the contents of messages that are to be exchanged by the gate terminal 101 or the merchant terminal 102 or 103 and the service providing system.

[1479] When data to be accessed is located at the remote address, the gate terminal 101 or the merchant terminal 102 or 103 generates a remote access request 5700, i.e., a message requesting that the merchant processor in the service providing system 110 access data, and transmits it to the merchant processor.

[1480] As is shown in Fig. 86A, a digital signature 8605 of a merchant is provided for data that consist of a remote access header 8600, which is header information indicating the message is the remote access request 5700 and describing the data structure of the request; a data address 8601, which indicates a remote address; a gate ID or an accounting machine ID 8602; a merchant ID 8603; and an issued time 8604, which indicates the date on which the remote access request 5700 was issued. The data are closed and are addressed to the service provider, thereby providing the remote access request 5700.

[1481] The merchant processor in the service providing system 110 receives the remote access request 5700, decrypts it and examines the digital signature, and generates a remote access data message 5701 and transmits it to the gate terminal 101 or to the merchant terminal 102 or 103.

[1482] As is shown in Fig. 86B, a digital signature of a service provider is provided for data that consist of a remote access header 8609, which is header information indicating that the message is the remote access data 5701 and describing the data structure of the remote access data; data that are requested 8610; a service provider ID 8611; and an issued time 8612, which indicates the date on which the remote access data 5701 was issued. The data are closed and are addressed to the merchant, thereby providing the remote access data 5701.

[1483] The gate terminal 101 or the merchant terminal 102 or 103 receives the remote access data 5701, decrypts it and examines the digital signature, stores it in the temporary area, and accesses the data.

[1484] Next, an explanation will be given for the contents of messages that the mobile user terminal 100, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 (automatic vending machine 104) and the electronic telephone accounting machine 800 (switching center 105) exchange with the service providing system 110 during the data updating process. The data updating process is a process whereby the service providing system updates the data in the RAM 1502 of the mobile user terminal 100, or the RAM and the hard disk of the merchant terminal 102, the merchant terminal 103 or the accounting machine 3555 (automatic vending machine 104). This process is hereinafter called a data updating process.

[1485] In Fig. 56B is shown the data updating process performed by the mobile user terminal 100, and in

Figs. 87A to 87E are shown the contents of messages that the mobile user terminal 100 exchanges with the service providing system 110.

[1486] When the value held by the clock counter matches the value in the update time register, the mobile user terminal 100 begins the data updating process. The mobile user terminal 100 generates a data update request 5602, i.e., a message requesting that the user processor of the service providing system 110 update data, and transmits it to the user processor.

[1487] As is shown in Fig. 87A, a digital signature of a user is provided for data that consists of a data update request header 8700, which is header information indicating the message is the data update request 5602 and describing the data structure of the request 5602; a user ID 8701; and an issued time 8702, which indicates the date on which the data update request 5602 was issued. The data are closed and are addressed to the service provider, thereby providing the data update request 5602.

[1488] The user processor of the service providing system 110 receives the data update request 5602, decrypts it and examines the digital signature, and generates a data update request response 5603, i.e., a message indicating the range of data to be uploaded, and transmits it to the mobile user terminal 100.

[1489] As is shown in Fig. 87B, a digital signature of a service provider is provided for data that consists of a data update request response header 8707, which is header information indicating that the message is the data update request response 5603, and describing the data structure of the response 5603; an update option code 8708 indicating the range of data to be uploaded; a service provider ID 8709; and an issued time 8710, which indicates the date on which the data update request response 5603 was issued. The data are closed and are addressed to the user, thereby providing the data update request response 5603.

[1490] The update option code 8708 is code information that indicates the range of data to be uploaded from the mobile user terminal to the service providing system. This code is employed to designate data for changing the service data area, data for changing the service data area and the user area, all the data in the service data area, all the data in the service data area and the user area, or all the data in the basic program area, the service data area and the user area. The update option code 8708 is designated by the user processor in the service providing system, and the same code is not always designated each time.

[1491] The mobile terminal 100 receives the data update request response 5603, decrypts it and examines the digital signature, and generates data that are designated with the update option code 8708. Then, the mobile user terminal 100 generates upload data 5604, i.e., a message that indicates the data that are to be uploaded to the service providing system 110, and transmits the data to the service providing system.

[1492] If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5604.

[1493] As is shown in Fig. 87C, a digital signature of a user is provided for data that consists of an upload data header 8715, which is header information indicating that the message is the upload data 5604 and describing the data structure; an upload packet number 8716 indicating a packet number for each of a plurality of packets; compressed upload data 8717 that are obtained by compressing the data that are to be uploaded to the service providing system; a user ID 8718; and an issued time 8719, which indicates the date on which the upload data 5604 was issued. The data are closed and are addressed to the user, thereby providing the upload data 5604.

[1494] The user processor of the service providing system receives the upload data 5604, and decrypts it and examines the digital signature. Then, the user processor decompresses the compressed upload data 8717 and compares the obtained data with the terminal data 4607 in the user information server 902 and the other data managed in the user data management information 4600. Then, the user processor generates update data 5605, which is a message for the updating of data in the RAM 1502 of the mobile user terminal 100, and transmits them to the mobile user terminal 100. If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5605.

[1495] As is shown in Fig. 87D, a digital signature of a service provider is provided for data that consists of an update data header 8724, which is header information indicating that the message is the update data 5605 and describing the data structure; an update packet number 8725 indicating a packet number when the data are divided into a plurality of packets; compressed update data 8726 that are obtained by

compressing update data; a service provider ID 8727; and an issued time 8728, which indicates the date on which the update data 5605 was issued. The data are closed and are addressed to the user, thereby providing the update data 5605.

[1496] The mobile user terminal 100 receives the update data 5605, decrypts it and examines the digital signature, decompresses the update data 8726, and updates the data in the RAM 1502.

[1497] In order to generate data for updating the RAM 1502, when there is no extra space in the object data area of the mobile user terminal 100, the user processor of the service providing system 110 compares the access times for the individual credit cards in the credit card list, and assigns a local address to the object data address for the credit card for which the access time is the latest; compares the access times for the individual tickets in the ticket list, and assigns a local address to the electronic ticket address for the ticket for which the access time is the latest; compares the access times for the individual payment cards in the payment card list, and assigns a local address to the electronic payment card address for the payment card for which the access time is the latest; compares the access times for the individual telephone cards in the telephone card list, and assigns a local address to the electronic telephone card address for the telephone card for which the access time is the latest; and compares the use times of the information items and assigns a local address to the use information address for the information for which the use time is the latest. When the version of the program of the mobile user terminal must be upgraded, the data in the basic program area are updated.

[1498] When the user processor of the service providing system 110 compares the upload data and finds an illegal alteration of data, the user processor generates, instead of the update data 5605, a mandatory expiration instruction 5605' that is a message for halting the function of the mobile user terminal 100, and transmits the instruction 5605' to the mobile user terminal 100.

[1499] As is shown in Fig. 87E, a digital signature of a service provider is provided for data that consists of a mandatory expiration header 8733, which is header information indicating that the message is the mandatory expiration instruction 5605' and describing the data structure; a service provider ID 8734; and an issued time 8735, which indicates that the date on which the mandatory expiration instruction 5605' was issued. The data are closed and are addressed to the user, thereby providing the mandatory expiration instruction 5605'.

[1500] Upon receipt of the mandatory expiration instruction 5605', the mobile user terminal 100 decrypts it and examines the digital signature, and changes the terminal status 1802 to "use disabled." As a result, the use of the mobile user terminal 100 is inhibited.

[1501] Through the data updating process, information that is comparatively frequently used is stored in the RAM of the mobile user terminal, the latest version of the program is maintained for the mobile user terminal, and the illegal alteration of the terminal data can be prevented.

[1502] In Fig. 57B is shown the data updating process performed by the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 (automatic vending machine 104) and the electronic telephone card accounting machine 800 (switching center 105), and in Figs. 88A to 88E are shown the contents of messages that are exchanged by the service providing system 110 and the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800.

[1503] When the value held by the clock counter matches the value in the update time register, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 begins the data updating process. The gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 generates a data update request 5702, i.e., a message requesting that the merchant processor of the service providing system 110 update data, and transmits it to the merchant processor.

[1504] As is shown in Fig. 88A, a digital signature of a merchant (communication service provider) is provided for data that consists of a data update request header 8800, which is header information indicating the message is the data update request 5702 and describing the data structure of the request 5702; an accounting ID (or a gate ID for the gate terminal) 8801; a merchant ID 8802 (a communication service provider ID for the electronic telephone card accounting machine) 8802; and an issued time 8803, which

indicates the date on which the data update request 5702 was issued. The data are closed and are addressed to the service provider, thereby providing the data update request 5702.

[1505] The merchant processor of the service providing system 110 receives the data update request 5702, decrypts it, examines the digital signature, generates a data update request response 5703, i.e., a message indicating the range of data to be uploaded, and transmits it to the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800.

[1506] As is shown in Fig. 88B, a digital signature of a service provider is provided for data that consists of a data update request response header 8808, which is header information indicating that the message is the data update request response 5703, and describing the data structure of the response 5703; an update option code 8809 indicating the range of data to be uploaded; a service provider ID 8810; and an issued time 8811, which indicates that the date on which the data update request response 5703 was issued. The data are closed and are addressed to the merchant (communication service provider for the electronic telephone card accounting machine), thereby providing the data update request response 5703.

[1507] The update option code 8809 is code information that indicates the range of data to be uploaded to the service providing system. This code is employed to designate data for changing the service data area, data for changing the service data area and the merchant area, all the data in the service data area, all the data in the service data area and the merchant area, or all the data in the basic program area, the service data area and the merchant area. The update option code 8809 is designated by the merchant processor in the service providing system, and the same code is not always designated each time.

[1508] The gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 receives the data update request response 5703, decrypts it and examines the digital signature, and generates data that are designated with the update option code 8809. Then, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 generates upload data 5704, i.e., a message that indicates to upload the data to the service providing system 110, and transmits the data to the service providing system.

[1509] If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5704.

[1510] As is shown in Fig. 88C, a digital signature of a merchant (communication service provider) is provided for data that consists of an upload data header 8816, which is header information indicating that the message is the upload data 5704 and describing the data structure; an upload packet number 8817 indicating a packet number for each of a plurality of packets; compressed upload data 8818 that are obtained by compressing the data that are to be uploaded to the service providing system; an accounting machine ID (gate ID for the gate terminal) 8819; a merchant (communication service provider) ID 8820; and an issued time 8821, which indicates the date on which the upload data 5704 was issued. The data are closed and are addressed to the merchant (communication service provider), thereby providing the upload data 5704.

[1511] The merchant processor of the service providing system receives the upload data 5704, and decrypts it and examines the digital signature. Then, the merchant processor decompresses the compressed upload data 8818 and compares the obtained data with the memory data 4705 in the merchant information server 903 and the other data managed in the merchant data management information 4700. Then, the merchant processor generates update data 5705, which is a message for updating data in the RAM and on the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800, and transmits them thereto. If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5705.

[1512] As is shown in Fig. 88D, a digital signature of a service provider is provided for data that consists of an update data header 8826, which is header information indicating that the message is the update data 5705 and describing the data structure; an update packet number 8827 indicating a packet number when the data are divided into a plurality of packets; compressed update data 8828 that are obtained by compressing update data; a service provider ID 8829; and an issued time 8830, which indicates the date on which the update data 5705 was issued. The data are closed and are addressed to the merchant

(communication service provider), thereby providing the update data 5705.

[1513] The gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 receives the update data 5705, decrypts it and examines the digital signature, decompresses the update data 8828, and updates the data in the RAM and on the hard disk.

[1514] In order to generate data for updating, when there is no extra space in the object data area or in the hard disk, the merchant processor of the service providing system 110 compares the transaction times for the history information in the transaction list, and assigns a local address to the transaction information address for history information for which the transaction time is the latest. When the version of the program of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 must be upgraded, the data in the basic program area are updated.

[1515] When the merchant processor of the service providing system 110 compares the upload data and finds the illegal alteration of the data, the merchant processor generates, instead of the update data 5705, a mandatory expiration instruction 5705', which is a message for halting the function of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800, and transmits the instruction 5705' thereto.

[1516] As is shown in Fig. 88E, a digital signature of a service provider is provided for data that consists of a mandatory expiration header 8835, which is header information indicating that the message is the mandatory expiration instruction 5705' and describing the data structure; a service provider ID 8836; and an issued time 8837, which indicates that the date on which the mandatory expiration instruction 5705' was issued. The data are closed and are addressed to the user, thereby providing the mandatory expiration instruction 5705'.

[1517] Upon receipt of the mandatory expiration instruction 5705', the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 decrypts it and examines the digital signature, and changes the terminal status (or the accounting machine status) to "use disabled." As a result, the use of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800 is inhibited.

[1518] Through the data updating process, information that is comparatively frequently used is stored in the RAM and on the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800, the latest version of the program is maintained for the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800, and the illegal alteration of the terminal data can be prevented.

[1519] An explanation will now be given for the contents of messages that the mobile user terminal 101 and the merchant terminal 102 exchange with the service providing system 110 during the processing for forcibly updating data. During the processing for forcibly updating data, upon the need of urgent data dating, the service providing system 110 forcibly updates the contents of the RAM 1502 of the mobile user terminal 101, or the contents of the RAM and the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 or the electronic telephone card accounting machine 800. This process is hereinafter called a forcible data updating process.

[1520] In Fig. 56C is shown the forcible data updating process performed by the mobile user terminal 100, and in Figs. 87C to 87F are shown the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110.

[1521] When the data in the RAM of the mobile user terminal 100 must be urgently updated, such as when the terms of a contract with the user are changed, the service providing system 110 generates a data update instruction 5606, i.e., a message instructing the mobile user terminal 100 to perform the forcible data updating process, and transmits it to the mobile user terminal 100.

[1522] As is shown in Fig. 87F, the digital signature of a service provider is provided for data that consists of a data update instruction header 8740, which is header information indicating that the message is the

data update instruction 5606 and describing the data structure; an update option code 8741; a service provider ID 8742; and an issued time 8743, which indicates the date on which the data update instruction 5606 was issued. These data are closed and addressed to the user, thereby providing the data update instruction 5606.

[1523] Upon receiving the data update instruction 5606, the mobile user terminal 100 decrypts it and examines the digital signature, and generates data as designated by the update option code 8741. Then, the mobile user 100 generates upload data 5607, which is a message for uploading the data to the service providing system 110, and transmits the data 5607 to the service providing system.

[1524] If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5607.

[1525] The user processor of the service providing system 110 receives the upload data 5607, decrypts it and examines the digital signature, decompresses the compressed upload data 8717 and compares the obtained data with the terminal data 4607 in the user information server 902 and the other data in user data management information 4600. Then, the service providing system 110 generates the update data 5608, which is a message for updating data in the RAM 1502 of the mobile user terminal 100, and transmits them to the mobile user terminal 100. If a large volume of data is to be transmitted to the mobile user terminal 100, the data are divided into a plurality of packets, which are transmitted as update data 5608.

[1526] The mobile user terminal 100 receives the update data 5608, decrypts it, examines the digital signature, decompresses the compressed update data 8726, and updates the data in the RAM 1502.

[1527] When the user processor of the service providing system compares the upload data with the other data and finds the illegal alteration of the data, the user processor generates, instead of the update data 5608, a mandatory expiration instruction 5608', which is a message for halting the function of the mobile user terminal 100, and transmits the instruction 5608' to the mobile user terminal 100.

[1528] Upon receipt of the mandatory expiration instruction 5608', the mobile user terminal 100 decrypts it, examines the digital signature, and changes the terminal status 1802 to "use disabled." As a result, the use of the mobile user terminal 100 is inhibited.

[1529] In Fig. 57C is shown the forcible data updating process performed by the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555 (automatic vending machine 104) and the electronic telephone card accounting machine (switching center 105). In Figs. 88C to 88F are shown the contents of messages that are exchanged by the service providing system 110 and the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800.

[1530] When the data in the RAM and on the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800 must be urgently updated, such as when the contents of a ticket is changed or the terms of a contract entered into by the service provider and the merchant (the communication service provider for the electronic telephone card accounting machine 800) are changed, the service providing system 110 begins the forcible data updating process.

[1531] First, the merchant processor of the service providing system 110 generates a data update instruction 5706, i.e., a message instructing the performance of the forcible data updating process, and transmits it to the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800.

[1532] As is shown in Fig. 88F, the digital signature of a service provider is provided for data that consists of a data update instruction header 8842, which is header information indicating that the message is the data update instruction 5706 and describing the data structure; an update option code 8843; a service provider ID 8844; and an issued time 8845, which indicates the date on which the data update instruction 5706 was issued. These data are closed and addressed to the user, thereby providing the data update instruction 5706.

[1533] Upon receiving the data update instruction 5706, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting

machine 800 decrypts it, examines the digital signature, and generates data as designated by the update option code 8843. Then, the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800 generates upload data 5707, which is a message for uploading the data to the service providing system 110, and transmits the data 5707 to the service providing system.

[1534] If a large volume of data is to be uploaded to the service system, the data are divided into a plurality of packets, which are transmitted as upload data 5707.

[1535] The merchant processor of the service providing system receives the upload data 5707, and decrypts it and examines the digital signature. The merchant processor then decompresses the compressed upload data 8818 and compares the obtained data with the memory data 4705 in the merchant information server 903 and the other data in merchant data management information 4700. Then, the merchant processor generates the update data 5708, which is a message for updating data in the RAM and on the hard disk of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800, and transmits them thereto. If a large volume of data is to be transmitted to the mobile user terminal 100, the data are divided into a plurality of packets, which are transmitted as update data 5708.

[1536] The gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800 receives the update data 5708, decrypts it and examines the digital signature, decompresses the compressed update data 8828, and updates the data in the RAM and on the hard disk.

[1537] When the merchant processor of the service providing system compares the upload data with the other data and finds the illegal alteration of data, the merchant processor generates, instead of the update data 5708, a mandatory expiration instruction 5708', which is a message for halting the function of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800, and transmits the instruction 5708' thereto.

[1538] Upon receipt of the mandatory expiration instruction 5708', the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800 decrypts it and examines the digital signature, and changes the terminal statue (or the accounting machine status) to "use disabled." As a result, the use of the gate terminal 101, the merchant terminal 102, the merchant terminal 103, the accounting machine 3555, or the electronic telephone card accounting machine 800 is inhibited.

[1539] An explanation will now be given for the contents of messages that the mobile user terminal 100 and the merchant terminal 104 exchange with the service providing system 110 during the processing for the data backup. During this processing, when the remaining battery capacity of the mobile user terminal 100 is small, the contents of the RAM are automatically backed up in the user information server of the service providing system. This process is hereinafter called a data backup process.

[1540] In Fig. 56D is shown the data backup process performed by the mobile user terminal 100, and in Figs. 87A to 87E are shown the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110. The data backup process is performed in substantially the same manner as is the data updating process. In the backup process, when the mobile user terminal 100 receives the update data 5612 and updates the data in the RAM 1502, the terminal 100 changes the terminal status 1802 to "writing disabled," and inhibits the input of new data to the RAM until there is an adequate available battery capacity.

[1541] When the battery capacity is reduced until it is equal to or smaller than Q, the mobile user terminal 100 generates a data backup request 5609, i.e., a message requesting that the user processor of the service providing system 110 perform the data backup process, and transmits it to the user processor.

[1542] The user processor of the service providing system receives the data update request 5609, decrypts it and examines the digital signature, and generates a data update request response 5610, i.e., a message indicating the range of data to be uploaded, and transmits it to the mobile user terminal 100.

[1543] The mobile user terminal 100 receives the data update request response 5610, decrypts it and examines the digital signature, and generates data designated by the update option code 8708. Then, the

mobile user terminal 100 generates upload data 5611, i.e., a message that indicates to upload the data to the service providing system 110, and transmits the data 5611 to the service providing system 110.

[1544] The user processor of the service providing system 110 receives the upload data 5611, decrypts it, and examines the digital signature. Then, the user processor decompresses the compressed upload data 8717, and compares the obtained data with the terminal data 4607 in the user information server 902 and the other data in the user data management information 4600. Then, the user processor generates the update data 5612, which is a message for updating data in the RAM 1502 of the mobile user terminal 100, and transmits them to the mobile user terminal 100.

[1545] The mobile user terminal 100 receives the update data 5612, decrypts it and examines the digital signature, decompresses the compressed update data 8726, and updates the data in the RAM 1502. In addition, the mobile user terminal 100 changes the terminal status 1802 to "writing disabled," and inhibits the entry of new data in the RAM until there is an adequate battery capacity.

[1546] When the user processor of the service providing system compares the upload data with the other data and finds the illegal alteration of data, the service providing system 110 generates, instead of the update data 5612, a mandatory expiration instruction 5612', which is a message for halting the function of the mobile user terminal 100, and transmits the instruction 5612' to the mobile user terminal 100.

[1547] Upon receipt of the mandatory expiration instruction 5612', the mobile user terminal 100 decrypts it, examines the digital signature, changes the terminal status 1802 to "use disabled" and "writing disabled." As a result, the use of the mobile user terminal 100 is inhibited.

[1548] Similarly, in Fig. 57D is shown the data backup process performed by the merchant terminal 103, and in Figs. 88A to 88E are shown the contents of messages that are exchanged by the merchant terminal 103 and the service providing system 110. The data backup process is performed in substantially the same manner as for the data updating process. In the backup process, when the merchant terminal 103 receives the update data 5712 and updates the data in the RAM 3002, the merchant terminal 103 changes the terminal status 3302 to "writing disabled," and inhibits the input of new data to the RAM until there is an adequate available battery capacity.

[1549] When the battery capacity is reduced until it is equal to or smaller than Q, the merchant terminal 103 generates a data backup request 5709, i.e., a message requesting that the merchant processor of the service providing system 110 perform the data backup process, and transmits it to the merchant processor.

[1550] The merchant processor of the service providing system receives the data update request 5709, decrypts it and examines the digital signature, and generates a data update request response 5710, i.e., a message indicating the range of data to be uploaded, and transmits it to the merchant terminal 103.

[1551] The merchant terminal 103 receives the data update request response 5710, decrypts it, examines the digital signature, and generates data designated by the update option code 8809. Then, the merchant terminal 103 generates upload data 5711, i.e., a message that indicates to upload the data to the service providing system 110, and transmits the data 5711 to the service providing system.

[1552] The merchant processor of the service providing system receives the upload data 5711, decrypts and it and examines the digital signature. Then, the merchant processor decompresses the compressed upload data 8818, and compares the obtained data with the memory data 4705 in the merchant information server 903 and the other data in the merchant data management information 4700. Then, the merchant processor generates the update data 5712, which is a message for updating data in the RAM 3002 of the merchant terminal 103, and transmits them to the merchant terminal 103.

[1553] The merchant terminal 103 receives the update data 5712, decrypts it and examines the digital signature, decompresses the compressed update data 8826, and updates the data in the RAM 3002. In addition, the merchant terminal 103 changes the terminal status 3302 to "writing disabled," and inhibits the entry of new data in the RAM until there is an adequate battery capacity.

[1554] When the merchant processor of the service providing system compares the upload data with the other data and finds the illegal alteration of the data, the merchant processor generates, instead of the update data 5712, a mandatory expiration instruction 5712', which is a message for halting the function of the merchant terminal 103, and transmits the instruction 5712' to the merchant terminal 103.

[1555] Upon receipt of the mandatory expiration instruction 5712', the merchant terminal 103 decrypts it and examines the digital signature, and changes the terminal status 3302 to "use disabled" and "writing disabled." As a result, the use of the merchant terminal 103 is inhibited.

[1556] An explanation will now be given for the contents of messages that are exchanged by devices during the ticket order processing.

[1557] In Fig. 58 are shown the procedures used for exchanging messages by the devices during the ticket order processing, and in Figs. 89A and 89B and Figs. 90A and 90B are shown the contents of messages that are exchanged by devices during the ticket order processing.

[1558] First, when a user displays the ticket order screen on the mobile user terminal 100 and performs a ticket order operation 5800, the mobile user terminal transmits a ticket order 5801 to the service providing system via digital wireless telephone communication.

[1559] As is shown in Fig. 89A, the digital signature of a user is provided for data that consists of a ticket order header 8900, which is header information indicating that the message is the ticket order 5801 and indicating the data structure; a service code 8901, which identifies the type of service requested by the user; a ticket order code 8902, which identifies the order code of a ticket entered by the user; a desired ticket date 8903; a desired number of tickets 8904; a request number 8905, which is arbitrarily generated as a number that uniquely represents the ticket order processing; a user ID 8906; and an issued time 8907, which indicates the date on which the ticket order 5801 is issued. These data are closed and addressed to the service providing system, thereby providing the ticket order 5801. The service code 8901 identifies the ticket order for a ticket issuer selected by the user.

*[1560] Upon receiving the ticket order 5801, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group for processing a ticket order 8908. The service director processor refers to the ticket issuer list 5203 and generates a ticket order 8920 for the ticket issuer identified by the service code 8901. The ticket issuer processor closes the ticket order 8920 and addresses it to the ticket issuer, and transmits the resultant order as a ticket order 11402 to the ticket issuing system 107.

[1561] As is shown in Fig. 89B, the digital signature of a service providing system is provided for data that consist of a ticket order header 8912, which is header information indicating that the message is the ticket order 5802 and describing the data structure; a ticket order code 8913; a desired ticket date 8914; a desired number of tickets 8915; a request number 8916; a customer number 8917, which uniquely identifies a user for the ticket issuer; a service provider ID 8918; and an issued time 8919, which indicates the date on which the ticket order 5802 was issued. These data are closed and addressed to the ticket issuer, thereby providing the ticket order 5802.

[1562] The customer number 8917 is identification information for a user that is useful only to the ticket issuer, and differs from the user ID or the telephone number. When there was a previous transaction to which the user and the ticket issuer were parties, the customer number that is registered in the customer table of the ticket issuer is designated. The customer table is indicated by using the customer table address 5230 of the ticket issuer list 5203.

[1563] Upon receiving the ticket order 5802, the ticket issuing system 107 decrypts it and examines the digital signature. The ticket issuing server 1100 employs the customer information in the customer information server 1101 and the ticket issuing condition of the ticket information server 1103 to generate a ticket order response 5803, which is a message prepared as a response to the ticket order 5802, and transmits it to the service providing system.

[1564] As is shown in Fig. 90A, the digital signature of a ticket issuer is provided for data that consists of a ticket order response header 9000, which is header information indicating that the message is the ticket order response 5803 and describing the data structure; a response code 9001, which identifies the type of response prepared for the ticket order 5802; a request number 9002; a customer number 9003; a ticket sales offer 9004, which constitutes an offer made by the ticket issuer to the user; an offer number 9005, which is an arbitrarily generated number that uniquely represents the offer made to the user; a validity term

9006 for the ticket sales offer 9004; a ticket issuer ID 9007; and an issued time 9008, which indicates the date on which the ticket order response 5803 was issued. These data are closed and addressed to the service provider, thereby providing the ticket order response 5803.

[1565] The response code 9001 identifies the type of response prepared for a ticket order, such as "ticket available," "sold out," "over ticket limit," or "ticket order code error."

[1566] The ticket sales offer 9004 is text information for the order received from the user, and includes the seat number for an available ticket or the price of a ticket. The digital signature of a ticket issuer is provided for the ticket sales offer. When a ticket can not be issued because all tickets have been sold, the ticket sales offer is not set.

[1567] The ticket issuing system 107 can specify a customer using the customer number 8917 that is included in the ticket order 5802. Before generating the ticket order response 5803, the ticket issuing system 107 can change the seat or the price of the ticket included in the ticket sales offer 9004 based on the purchase history of the customer.

[1568] Upon receiving the ticket order response 5803, the ticket issuer processor of the service providing system decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor uses a ticket order response 9009 to generate a ticket order response 9023. The user processor closes the ticket order response 9023 and addresses IT to the user, and transmits it as a ticket order response 5804 to the mobile user terminal.

[1569] As is shown in Fig. 90B, the digital signature of a service provider is provided for data that consists of a ticket order response header 9014, which is header information identifying the message as the ticket order response 5804 and describing the data structure; a response code 9015; a response message 9016, which comprises the contents of the response to the ticket order; a request number 9017; a ticket sales offer 9018; an offer number 9019; a validity term 9020 for the ticket sales offer 9018; a service provider ID 9021; and an issued time 9022, which indicates the date on which the ticket order response 5804 was issued. These data are closed and addressed to the user, thereby providing the ticket order response 5804.

[1570] The response message 9016 is a standardized text message that the service director processor sets in accordance with the response code 9001. When the response code 9001 is not code indicating "ticket available," a standardized message is prepared that comprises the contents of the response code.

[1571] Upon receiving the ticket order response 5804, the mobile user terminal decrypts it and examines the digital signature, and displays the contents of the ticket order response 5804 on the LCD 303. The ticket order processing is thereafter terminated. When the response code 9015 indicates "ticket available," the contents of the ticket sales offer 9018 are displayed. In the other cases, the response message 9016 is displayed.

[1572] An explanation will now be given for the contents of messages that are exchanged by devices during the ticket purchase processing.

[1573] In Fig. 59 are shown the procedures for the exchange of messages by devices during the ticket purchase processing. In Figs. 91A and 91B, 92A and 92B, 93A and 93B, 94A and 94B, and 95A and 95B are shown the contents of messages that are exchanged by devices during the ticket purchase processing.

[1574] First, when a user performs a ticket purchase order operation 5900, the mobile user terminal transmits a ticket purchase order 5901 to the service providing system through digital wireless telephone communication.

[1575] As is shown in Fig. 91A, the digital signature of a user is provided for data that consists of a ticket purchase order header 9100, which is header information identifying the message as the ticket purchase order 5901 and describing the data structure; a response code 9101, which identifies the type of service requested by the user; a ticket sales offer 9102, which is included in the ticket order response 5804; an offer number 9103, which identifies the ticket sales offer 9102; a payment service code 9104, which identifies a credit card designated by the user; a payment value 9105; a payment option code 9106, which identifies a payment option, such as the number of payments designated by the user; a request number 9107, which is an arbitrarily generated number that uniquely represents the ticket purchase processing; a

validity term 9108 for the ticket purchase order 5901; a user ID 9109; and an issued time 9110, which is the date on which the ticket purchase order 5901 was issued. These data are closed and addressed to the service provider, thereby providing the ticket purchase order 5901. The service code 9101 identifies the purchase of a ticket from a ticket issuer who issued the ticket sales offer 9102.

[1576] Upon receiving the ticket purchase order 5901, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group that processes a ticket order 8908. The service director processor refers to the ticket issuer list 5203 and generates a ticket purchase order for the ticket issuer indicated by the service code 9101. The ticket issuer processor closes the ticket order and addresses it to the ticket issuer, and transmits the resultant order as a ticket purchase order 5902 to the ticket issuing system 107.

[1577] As is shown in Fig. 91B, the digital signature of a service providing system is provided for data that consists of a ticket purchase order header 9115, which is header information indicating that the message is the ticket purchase order 5902 and describing the data structure; an offer number 9116, which identifies a ticket sales offer issued by the ticket issuer; a payment service code 9117; a payment value 9118; a payment option code 9119; a request number 9120; a customer number 9121, which uniquely represents a user for the ticket issuer; a validity term 9122 for the ticket purchase order 5902; a service provider ID 9123; and an issued time 9124, which is the date on which the ticket purchase order 5902 was issued. These data are closed and addressed to the ticket issuer, thereby providing the ticket purchase order 5902.

[1578] When there was a previous transaction to which the user and the ticket issuer were parties, a customer number that is registered in the customer table of the ticket issuer is established as the customer number 9121. When there was no previous transaction, the service director processor generates for the ticket issuer a number that uniquely represents the user, establishes it as the customer number 9121, and registers that number in the customer table. The customer table is designated by using the customer table address 5230 of the ticket issuer list 5203.

[1579] Upon receiving the ticket order 5902, the ticket issuing system 107 decrypts it and examines the digital signature. The ticket issuing server 1100 updates the data in the customer information server 1101, the ticket issuing information server 1102 and the ticket information server 1103, generates ticket data (9219) for the ordered ticket, and transmits, to the service providing system, an electronic ticket issuing commission 5903, which constitutes a message requesting the process for issuing an electronic ticket that corresponds to the ticket and the process for settling the price of the ticket.

[1580] As is shown in Fig. 92A, the digital signature of a ticket issuer is provided for data that consists of an electronic ticket issuing commission header 9200, which is header information identifying the message as the electronic ticket issuing commission 5903 and describing the data structure; a transaction number 9201, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 9202, which conveys the price of a ticket; a clearing option 9203, which indicates which clearing procedures apply; a request number 9204; a ticket code 9205, which identifies the type of electronic ticket that is to be issued; a template code 9206, which identifies a template program to be used for an electronic ticket that is to be issued; a number of tickets 9207, which indicates how many tickets are to be issued; ticket data 9208; representative component information 9209; a ticket issuer ID 9210; and an issued time 9210, which is the date on which the electronic ticket issuing commission 5903 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket issuing commission 5903.

[1581] The clearing option 9203 is information by which the ticket issuing system designates, to the service providing system, the procedures to be used for clearing the price of a ticket. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic ticket to a user after the price of the ticket has been cleared, and a delayed clearing process for clearing the price of a ticket after an electronic ticket has been issued. The clearing option 9203 is used to designate either clearing process.

[1582] In the delayed clearing process, since an electronic ticket is issued to a user before the clearing process Is performed, the user does not have to wait.

[1583] For example, based on a purchase history maintained for customers, the ticket issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known to be trustworthy, and can designate the spontaneous clearing for a customer with whom it has had no previous

dealings.

[1584] The ticket data 9208 is ticket information issued by the ticket issuer. A number of ticket information items equivalent to the number of tickets 9207 are established as the ticket data 9208. For one ticket, the digital signature of a ticket issuer is provided for data that consist of a ticket ID 9216, ticket information 9217 and a ticket issuer ID 9218, and the ticket information is thereby provided. The ticket information 9217 is ASCII information describing the contents of a ticket. For the ticket information 9217, the title of a ticket, the date, the location, the seat class, the sponsor and whether it can be transferred, and the usage condition information, such as the number of coupon tickets, when the ticket is used as a coupon ticket, are described using a form whereby tag information representing various information types is additionally provided.

[1585] The representative component information 9209 is information that is established as the representative component information 1932 for an electronic ticket to be generated. Therefore, the representative component information 9209 may not be set for use.

[1586] The ticket issuer processor of the service providing system receives the electronic ticket issuing commission 5903, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic ticket issuing process and the ticket price clearing process in accordance with the clearing procedures designated by using the clearing option 9203.

[1587] In Fig. 59 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1588] For the spontaneous clearing, the service director processor generates a clearing request 9324, which is a message requesting the clearing of the price of a ticket. The transaction processor processor closes the clearing request 9324 and addresses it to the transaction processor, and then transmits it as a clearing request 5904 to the transaction processing system 106.

[1589] As is shown in Fig. 93B, the digital signature of a service provider is provided for data that consists of a clearing request header 9314, which is header information indicating that the message is the clearing request 5904 and describing the data structure; a user clearing account 9315, which includes a credit card that corresponds to the payment service code designated by the user; a ticket issuer clearing account 9316, which designates the clearing account of a ticket issuer; a payment value 9317; a payment option code 9318; a request number 9319, which is issued by the mobile user terminal 100; a transaction number 9320, which is issued by the ticket issuing system; a validity term 9321, which presents the period during which the clearing request 5904 is effective; a service provider ID 9322; and an issued time 9323, which indicates the date on which the clearing request 5904 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 5904.

[1590] The transaction processing system 106 receives the clearing request 5904, decrypts it and examines the digital signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 5905, and transmits it to the service providing system 110.

[1591] As is shown in Fig. 94A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 9400, which is header information indicating that the message is the clearing completion notification 5905 and describing the data structure; a clearing number 9401, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 9402; a ticket issuer clearing account 9403; a payment value 9404; a payment option code 9405; a request number 9406; a transaction number 9407; clearing information 9408 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 9409 for a ticket issuer that is accompanied by the digital signature of the transaction processor; clearing information 9410 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 9411; and an issued time 9412, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 5905.

[1592] Upon receiving the clearing completion notification 5905, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9413 to the service director processor. Upon receiving the clearing completion notification 9413, the service director processor generates a clearing completion notification 9430 for the

ticket issuer. The ticket issuer processor closes the clearing completion notification 9430, and transmits it to the ticket issuing system 107 as a clearing completion notification 5906 for the ticket issuer.

[1593] As is shown in Fig. 94B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 9417, which is header information indicating that the message is the clearing completion notification 5906 and describing the data structure; a clearing number 9418; a customer number 9419; a ticket issuer ID 9420; a payment service code 9421; a payment value 9422; a payment option code 9423; a request number 9424; a transaction number 9425; clearing information 9426 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 9427; a service provider ID 9428; and an issued time 9429, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the ticket issuer, thereby providing the clearing completion notification 5906.

[1594] Upon receiving the clearing completion notification 5906, the ticket issuing system decrypts it and examines the digital signature, and generates a receipt 5907 and transmits it to the service providing system.

[1595] As is shown in Fig. 95A, the digital signature of a ticket issuer is provided for data that consists of a receipt header 9500, which is header information indicating that the message is the receipt 5907 and describing the data structure; a customer number 9501; ticket issuing information 9502; a payment service code 9503; a payment value 9504; a payment option code 9505; a request number 9506; a transaction number 9507; clearing information 9508; a transaction processor ID 9509; a ticket issuer ID 9510; and an issued time 9511, which indicates the date on which the receipt 5907 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 5907. The ticket issuing information 9502 is information concerning the ticket issuing process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1596] Upon receiving the receipt 5907, the ticket issuer processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 9512 to the service director processor. The service director processor employs the receipt 9512 to generate a receipt 9523 for a user.

[1597] In addition, the service director processor generates a clearing completion notification 9430 for the ticket issuing system, generates an electronic ticket to be issued to the user, and further generates an electronic ticket issuing message 9227 that includes the electronic ticket that is generated.

[1598] The user processor closes the electronic ticket issuing message 9227 and the receipt 9523 while addressing them to the user, and transmits them as an electronic ticket issuing message 5908 and a receipt 5909 to the mobile user terminal 100 via digital wireless communication.

[1599] As is shown in Fig. 92B, the digital signature of a service provider is provided for data that consist of an electronic ticket issuing header 9220, which is header information indicating that the message is the electronic ticket issuing message 5908 and describing the data structure; a transaction number 9221; a request number 9222; the number of tickets 9223; electronic ticket data 9224 that are generated; a service provider ID 9225; and an issued time 9226, which indicates the date on which the electronic ticket issuing message 5908 was issued. These data are closed and addressed to the user, thereby providing the electronic ticket issuing message 5908. The electronic ticket data 9224 includes electronic tickets 9231 equivalent in number to the number of tickets 9223.

[1600] As is shown in Fig. 95B, the digital signature of a service provider is provided for data that consists of a receipt header 9516, which is header information indicating that the message is the receipt 5909 and describing the data structure; a user ID 9517; a receipt 9518 (9512) obtained by decryption; clearing information 9519 for a user that is accompanied by the digital signature of a transaction processor; ticket issuing information 9520; a service provider ID 9521; and an issued time 9522, which indicates the date on which the receipt 5909 was issued. These data are closed and addressed to the user, thereby providing the receipt 5909. The ticket issuing information 9520 is information for the electronic ticket issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1601] Upon receiving the electronic ticket issuing message 5908 and the receipt 5909, the mobile user terminal decrypts them and examines the digital signatures, enters in the ticket list 1712 an electronic ticket included in the electronic ticket issuing message 5908, enters the receipt 9523 in the use list 1715, and

displays the electronic ticket on the LCD 303.

[1602] The generation of an electronic ticket by the service director processor is performed as follows.

[1603] First, the service director processor refers to the electronic ticket template list 4905 for the ticket issuer that is stored in the ticket issuer information server. Then, by using the electronic ticket template program that is identified by the template code 9206 of the electronic ticket issuing commission 5903, the service director processor generates a ticket program for an electronic ticket. Specifically, the ticket program data 1913 for an electronic ticket are generated using the transaction module and the display module, which are described as being located at the transaction module address 4919, and the display module address 4920 in the electronic ticket template list 4905, and the representative component information 9209 in the electronic ticket issuing commission 5903. When the representative component information 9209 is not present in the electronic ticket issuing commission 5903, the default representative component information located at the default representative component information address 4921 is employed as the information for an electronic ticket.

[1604] Following this and based on the usage condition information included in the ticket information 9217, the service director processor generates the ticket status 1907 and the variable ticket information 1908. Whether the ticket status 1907 can be transferred is designated, and when the ticket is used as a coupon ticket, the number of coupons is employed as the variable ticket information 1907. The service director processor generates a new pair consisting of a ticket signature private key and a ticket signature public key, and further generates the ticket program 1901 for an electronic ticket by employing the ticket private key and the gate public key that are registered in the electronic ticket management information 5300.

[1605] Furthermore, the service director processor generates an electronic ticket by employing the obtained ticket signature public key to generate the certificate 1903 for the electronic ticket, and by employing the ticket data 9219 in the electronic ticket issuing commission 5903 to generate the presentation ticket 1902 for the electronic ticket.

[1606] The procedures for the delayed clearing will now be described.

[1607] In Fig. 60 are shown the procedures for exchanging messages between the devices in the ticket purchase process for the delayed clearing. The same process is performed as is used for the spontaneous clearing until the ticket issuing system transmits the electronic ticket issuing commission to the service providing system.

[1608] When the delayed clearing is designated by the clearing option 9203, the service director processor generates an electronic ticket to be issued to the user, and also generates the electronic ticket issuing message 9227, which includes the generated electronic ticket, and a temporary receipt message 9310, which corresponds to a temporary receipt. The generation of the electronic ticket is performed in the same manner as that used for the spontaneous clearing.

[1609] The user processor closes the electronic ticket issuing message 9227 and the temporary receipt 9310 and addresses them to the user, and transmits these messages as an electronic ticket issuing message 6004 and a temporary receipt 6005 to the mobile user terminal 100 via digital wireless telephone communication.

[1610] As is shown in Fig. 93A, the digital signature of a service provider is provided for data that consists of a temporary receipt header 9300, which is header information indicating that the message is the temporary receipt 6005 and describing the data structure; a user ID 9301; ticket issuing information 9302; a payment service code 9303; a payment value 9304; a payment option code 9305; a request number 9306; a transaction number 9307; a service provider ID 9308; and an issued time 9309, which indicates the date on which the temporary receipt 6005 was issued. These data are closed and addressed to the user, thereby providing the temporary receipt 6005. The ticket issuing information 9302 is information concerning the electronic ticket issuing process that is performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1611] The data structure of the electronic ticket issuing message 6004 is the same as that used for the electronic ticket issuing message 5908.

[1612] Upon receiving the electronic ticket issuing message 6004 and the temporary receipt 6005, the

mobile user terminal decrypts them and examines the digital signatures, enters an electronic ticket included in the electronic ticket issuing message 6004 in the ticket list 1712, enters the temporary receipt 9310 in the use list 1715, and displays the electronic ticket on the LCD 303.

[1613] Following this, the service director processor performs the clearing process for the price of the ticket. First, the service director processor generates a clearing request 9324, which is a message requesting the performance of the clearing process for the price of the ticket. The transaction processor closes the clearing request 9324 and addresses it to the transaction processor, and transmits it as a clearing request 6007 to the transaction processing system 106.

[1614] Upon receiving the clearing request 6007, the transaction processing system 106 decrypts it and examines the digital signature, and performs the clearing process. The transaction processing system 106 generates a clearing completion notification 6008 and transmits it to the service providing system 110.

[1615] Upon receiving the clearing completion notification 6008, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9413 to the service director processor. The service director processor employs the received clearing completion notification 9413 to generate a clearing completion notification 9430 for the ticket issuer. And the ticket issuer processor closes the clearing completion notification 9430 and transmits it to the ticket issuing system 107 as a clearing completion notification 6009 for the ticket issuer.

[1616] The ticket issuing system decrypts the received clearing completion notification 6009 and examines the digital signature, and generates a receipt 6010 and transmits it to the service providing system.

[1617] The ticket issuer processor of the service providing system decrypts the received receipt 6010 and examines the digital signature, and transmits a receipt 9512 to the service director processor. The service director processor employs the receipt 9512 to generate a receipt 9523 for a user.

[1618] The receipt 9523 that is generated is not immediately transmitted to the mobile user terminal 100 of the user. When the mobile user terminal has performed the data updating process, the user processor replaces the temporary receipt 9310 in the use list 1715 with the receipt 9523, and transmits the receipt 9523 as one part of the update data 6011 to the mobile user terminal 100.

[1619] The data structures of the clearing request 6007, the clearing completion notification 6008, the clearing completion notification 6009 and the receipt 6010 for the delayed clearing are the same as those provided for the clearing request 5904, the clearing completion notification 5905, the clearing completion notification 5906 and the receipt 5907 for the spontaneous clearing.

[1620] The delayed clearing process need not be performed immediately after the electronic ticket is issued, and together with the other clearing processes, may be performed, for example, once a day.

[1621] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110 during the ticket registration processing.

[1622] In Fig. 65A are shown the procedures for exchanging messages between devices in the ticket registration processing, and in Figs. 106A and 106B are shown the contents of messages that are exchanged by the devices in the ticket registration processing.

[1623] First, when the user performs an electronic ticket registration operation 6500, the mobile user terminal generates a ticket registration request 6501 and transmits it to the service providing system via digital wireless telephone communication.

[1624] As is shown in Fig. 106A, the digital signature of a user is provided for data that consists of a ticket registration request header 10600, which is header information indicating that the message is the ticket registration request 6501 and describing the data structure; a ticket ID 10601 of a ticket to be registered; a user ID 10602; and an issued time 10603, which indicates the date on which the ticket registration request 6501 was issued. These data are closed and addressed to the service provider, thereby providing the ticket registration request 6501.

[1625] The user processor of the service providing system decrypts the received ticket registration request 6501 and examines the digital signature, and transmits the request 6501 to the service manager processor.

The service manager processor generates a service director processor to form a process group that processes a ticket registration request 10604. The service director processor ascertains that the electronic ticket indicated by the ticket ID 10601 is registered in the ticket list 4610 for the user in the user information server 902, and registers that electronic ticket in the registered ticket list 5303 for electronic tickets of the service director information server 901. At this time, the service director processor newly generates a ticket signature private key and a ticket signature public key pair. Further, the service director processor generates a registered ticket certificate using the ticket signature public key, and registers it in the registered ticket list 5303. The service director processor then generates a ticket certificate issuing message 13313 using the ticket signature private key and the registered ticket certificate that has been generated. The user processor closes the ticket certificate issuing message 13313 and addresses it to the user, and transmits it as a ticket certificate issuing message 6502 to the mobile user terminal via digital wireless telephone communication.

[1626] As is shown in Fig. 106B, the digital signature of a service provider is provided for data that consists of a ticket certificate issuing header 10608, which is header information indicating that the message is the ticket certificate issuing message 6502 and describing the data structure; a ticket digital signature private key 10609; a registered ticket certificate 10610; a service provider ID 10611, and an issued time 10612, which indicates the date on which the ticket certificate issuing message 6502 was issued. These data are closed and addressed to the user, thereby providing the ticket certificate issuing message 6502.

[1627] The mobile user terminal 100 decrypts the received ticket certificate issuing message 6502 and examines the digital signature, replaces the ticket signature private key and the ticket certificate of an electronic ticket with the ticket signature private key 10609 and the registered ticket certificate 10610, both of which are included in the ticket certificate issuing message 6502, changes the registration state in the ticket status to the post-registration state, and displays on the LCD the electronic ticket that has been registered (display a ticket that is registered; 6503).

[1628] An explanation will now be given for the contents of messages that are exchanged by the gate terminal 101 and the service providing system 110 during the ticket setup processing.

[1629] In Fig. 66 are shown procedures for exchanging messages between the devices in the ticket setup processing performed when the merchant sets up, at the gate terminal 101, a ticket to be examined. In Figs. 109A and 109B are the contents of messages that are exchanged by the devices during the ticket setup processing.

[1630] First, when the operator (merchant) of the gate terminal 101 performs a ticket setup operation 6600, the gate terminal generates a ticket setup request 6601 and transmits it to the service providing system via digital telephone communication.

[1631] As is shown in Fig. 109A, the digital signature of a merchant is provided for data that consists of a ticket setup request header 10900, which is header information indicating that the message is the ticket setup request 6601 and describing the data structure; a ticket code 10901 entered by the merchant during the ticket setup operation 6600; a gate ID 10902 for the gate terminal; a merchant ID 10903; and an issued time 10904, which indicates the date on which the ticket setup request 6601 was issued. These data are closed and addressed to the service provider, thereby providing the ticket setup request 6601.

[1632] The merchant processor of the service providing system decrypts the received ticket setup request 6601 and examines the digital signature, and transmits the request 6601 to the service manager processor. The service manager processor generates a service director processor to form a process group that processes a ticket setup request 10605. The service director processor ascertains that a merchant is registered in the merchant list 5302 for the electronic ticket that is identified by the ticket code 10901 for the service director information server 901. Then, the service director processor generates a ticket setup message 10919 by referring to the electronic ticket management information 5300, which is stored in the service director information server 901 for the pertinent electronic ticket, and the electronic ticket template list 4905, which is stored in the ticket issuer information server 905 of the pertinent ticket issuer (the ticket issuer ID 5306). Specifically, the service director processor generates the ticket setup message 10919 by using the ticket examination module, which is located at the ticket examination module address 4922 in the electronic ticket template list 4905 that is identified by the template code 5312 of the electronic ticket management information 5300, and the ticket public key 5309 and the gate private key 5310, which are registered in the electronic ticket management information 5300. The merchant processor closes the ticket setup 10919 and addresses it to the merchant, and transmits it as a ticket setup message 6602 to the gate

terminal via digital telephone communication.

[1633] As is shown in Fig. 109B, the digital signature of a service provider is provided for data that consists of a ticket setup header 10909, which is header information indicating that the message is the ticket setup message 6602 and describing the data structure; a ticket name 10910 for an electronic ticket to be issued; a ticket code 10911; a ticket issuer ID 10912; a validity term 10913; a gate private key 10914; a ticket public key 10915; a ticket examination module 10916; a service provider ID 10917; and an issued time 10918, which indicates the date on which the ticket setup message 6602 was issued. These data are closed and addressed to the merchant, thereby providing the ticket setup message 6602.

[1634] The mobile user terminal decrypts the received ticket setup message 6602 and examines the digital signature, registers, in the ticket list 2409, electronic ticket examination program information that is included in the ticket setup message 6602, and displays on the touch panel LCD a message indicating that the ticket setup process has been completed (display the setup completion; 6603).

[1635] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the gate terminal 101 during the ticket examination processing.

[1636] In Fig. 67 are shown procedures for the exchange of messages by the devices during the ticket examination processing, and in Figs. 110A and 110B and Figs. 111A and 111B are the contents of the messages that are exchanged by the devices during the ticket examination processing.

[1637] First, when a user performs a ticket presentation operation 6700, the mobile user terminal generates a ticket presentation message 6701 by using an electronic ticket to be examined and an arbitrarily generated test pattern, and transmits it to the gate terminal via infrared communication.

[1638] As is shown in Fig. 110A, the ticket presentation message 6701 consists of a ticket presentation header 11000, which is header information indicating that the message is the ticket presentation message 6701 and describing the data structure; a service code 11001, which identifies the request for the examination of an electronic ticket; a request number 11002, which is an arbitrarily generated number that uniquely represents the ticket examination process; a ticket 11003 for presenting an electronic ticket to be examined; a ticket certificate 11004; the current ticket status of an electronic ticket that is to be examined; variable ticket information 11006; a ticket ID 11007; an issued time 11008, which indicates the date on which the ticket presentation message 6701 was issued; and a gate test pattern 11010, which is an arbitrarily generated test pattern. The digital signature is provided, using the ticket signature private key of an electronic ticket, for the ticket status 11005, the variable ticket information 11006, the ticket ID 11007 and the issued time 11008. The gate test pattern is encrypted using the gate public key.

[1639] The presentation ticket 11003, the ticket certificate 11004, the ticket status 11005, the variable ticket information 11006, the ticket ID 11007 and the issued date 11008 specify the contents of the electronic ticket for the gate terminal, and the gate test pattern 11010 is a test pattern for authorizing the gate terminal.

[1640] Upon receiving the ticket presentation message 6701, first, the gate terminal refers to the ticket list 2409, activates a ticket examination module that corresponds to the ticket code of the electronic ticket that is presentation, examines the validity of the contents of the ticket presentation message 6701, and generates a ticket examination message 6702 and transmits it to the mobile user terminal via infrared communication.

[1641] In the verification process for the validity of the ticket presentation message 6701, the gate terminal employs the fact that the ticket certificate 11004 is a registered ticket certificate and examines the ticket status 11005 and the variable ticket information 11006 to determine whether an electronic ticket that is to be examined is valid. Then, the gate terminal examines the presentation ticket 11003, the digital signature of the service provider that is provided for the ticket certificate 11004, and the validity term. Further, the gate terminal employs the ticket signature public key of the ticket certificate 11004 to examine the digital signature of the electronic ticket that is provided for the ticket status 11005, the variable ticket information 11006, the ticket ID 11007, and the issued time 11008. Thus, the validity of the ticket presentation message 6701 is verified.

[1642] In the generation of the ticket examination message 6702, the gate terminal decrypts the gate test pattern 11010 using the gate private key, and employs the ticket public key to encrypt the ticket test pattern

11108 that is arbitrarily generated.

[1643] As is shown in Fig. 110B, the digital signature of a merchant is provided for the data that consists of a ticket examination header 11012, which is header information indicating that the message is the ticket examination message 6702 and describing the data structure; a transaction number 11013; a response message 11014; a request number 11015; a ticket ID 11016; an instruction code 11017; a gate test pattern 11018, which is decrypted; a ticket test pattern 11019, which is an arbitrarily generated test pattern; a gate ID 11021; a merchant ID 11022; and an issued time 11023, which indicates the date on which the ticket examination message 6702 was issued. Thus, the ticket examination 6702 is provided. The ticket test pattern 11019 is encrypted using the ticket public key.

[1644] The transaction number 11013 is a number, arbitrarily generated by the gate terminal, that uniquely represents the ticket examination process. When, as a result of the examination of the ticket presentation message 6701, the ticket examination process can not be performed (the electronic ticket is one that can not be examined by the pertinent gate terminal), a value of 0 is set. When the ticket examination process can be performed, a value other than 0 is set.

[1645] The response message 11014 is text information constituting the message transmitted by the merchant to the user. When the gate terminal can not examine an electronic ticket that is presented (transaction number = 0), data to that effect is included in the response message. The response message is optionally set, and may not be reset.

[1646] The instruction code 11017 is command code information for an electronic ticket that indicates how the ticket status and variable ticket information of the electronic ticket can be changed. The instruction code is varied by combining the electronic ticket transaction module and the ticket examination module.

[1647] When the mobile user terminal receives the ticket examination message 6702, first, in order to verify the gate terminal the mobile user terminal compares the gate test pattern 11010 with the gate test pattern 11018 included in the ticket examination message 6702, and changes the ticket status and the variable ticket information of the electronic ticket in accordance with the instruction code 11017. Then, the mobile user terminal decrypts the ticket test patten using the ticket private key, generates a ticket examination response 6703, and transmits it to the gate terminal via infrared communication.

[1648] As is shown in Fig. 111A, the digital signature using the ticket signature private key and the digital signature of a user are provided for the data that consist of a ticket examination response header 11100, which is header information indicating that the message is the ticket examination response 6703 and describing the data structure; a ticket examination number 11101, which indicates the order of the ticket examination process; a ticket test pattern 11102, which is decrypted; a ticket status 11103 and variable ticket information 11104, which are modified; a gate ID 11105; a merchant ID 11106; a request number 11107; a transaction number 11108; a ticket code 11109; a ticket ID 11110; and an issued time 11111, which indicates the date on which the ticket examination response 6703 was issued. In this fashion, the ticket examination response 6703 is provided.

[1649] Upon receiving the ticket examination response 6703, first, the gate terminal authorizes the electronic ticket by comparing the ticket test pattern 111019 with the ticket test pattern 11102 that is included in the ticket examination response 6703, examines the validity of the contents of the ticket examination response 6703, and generates an examination certificate 6704 and transmits it to the mobile user terminal via infrared communication.

[1650] In the verification process for the validity of the ticket examination response 6703, the gate terminal determines whether the ticket status 11103 and the variable ticket information 11104 have been changed in accordance with the instruction code 11107, and examines the digital signature of the ticket examination response 6703.

[1651] As is shown in Fig. 111B, the digital signature of a merchant is provided for the data that consist of an examination certificate header 11113, which is header information indicating that the message is the examination certificate 6704 and describing the data structure; examination information 11114, which is text information indicating the contents of the ticket examination process; a ticket ID 11115; a request number 11116; a transaction number 11117; a ticket examination number 111187; a gate ID 11119; a merchant ID 11120; and an issued time 11121, which indicates the date on which the examination certificate 6704 was issued. In this fashion, the examination certificate 6704 is provided.

[1652] Upon receiving the examination certificate 6704, the mobile user terminal increments the ticket examination number, registers the examination certificate 6704 as usage information in the use list 1715, and displays the examined electronic ticket on the LCD (display the examined ticket; 6706).

[1653] When the gate terminal has transmitted the examination certificate 6704, the gate terminal registers, in the transaction list 2510, the ticket examination response 6703 as history information for the ticket examination process, and displays the results obtained during the ticket examination process on the touch panel LCD (display the results of examination; 6705). When the gate opening/closing device is connected to the gate terminal, the gate is automatically opened (entrance permission 6707).

[1654] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket reference processing.

[1655] In Fig. 71 are shown procedures for the exchange of messages by the devices during the ticket reference processing, and in Figs. 88A to 88D and Fig. 116A are shown the contents of messages that are exchanged during the ticket reference processing.

[1656] The ticket reference processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the gate terminal.

[1657] Therefore, for the ticket reference process, the procedures for the exchange of messages by the gate terminal and the service providing system, and the contents (data structures) of the messages to be exchanged are the same as those employed for the above described data updating processing.

[1658] Compressed upload data 8818 in the upload data 5702 include a ticket examination response that is newly registered in the transaction list 2510 during the ticket examination process conducted during the period extending from the previous performance of the data updating process to the current performance of the data updating process.

[1659] During the data updating processing, the merchant processor transmits, to the service manager processor, a message requesting the reference process be performed for the ticket examination response that is uploaded from the gate terminal. The service manager processor generates a service director processor to form a process group for examining the validity of the ticket examination response.

[1660] First, the service director processor determines whether the gate ID 11105 and the merchant ID 11106 in the ticket examination response match the gate ID 5215 of the merchant and the merchant ID 5214. Then, the service director processor examines the registered ticket list 5303 in the service director information server 901 to verify that the electronic ticket for which the ticket examination response was issued is registered. The service director processor employs the user public key 5323 to examine the digital signature of the user that accompanies the ticket examination response, and employs the registered ticket certificate to examine the digital signature for the ticket that accompanies the ticket examination response. In addition, the service director processor employs the ticket examination number when examining the matching of the ticket status with the variable ticket information that has been modified, and transmits the result of the examination to the merchant processor. As a result, the ticket examination response is registered in the ticket examination response list.

[1661] The merchant processor enters the received ticket reference results in the compressed update data 8828 in the update data 5705, and transmits the data 5705 to the gate terminal.

[1662] When an error occurs in the process for verifying the validity of the ticket examination response, the service director processor transmits a message indicating that an error occurred in the management system 908.

[1663] Upon receiving the update data 5705, the gate terminal decompresses the update data 8828 and updates the data in the RAM and on the hard disk. At this time, the ticket reference results are registered in the authorization report list 2511 of the gate terminal.

[1664] If the firm represented by the merchant differs from that represented by the ticket issuer and a payment is made by the ticket issuer to the merchant who handles the ticket, or if the usage of the ticket is

periodically reported to the ticket issuer in accordance with the terms of a contract, in accordance with the ticket examination response that is newly registered in the ticket examination response list, the service director processor generates weekly, for example, a usage condition notification 11606, which is a message for notifying the ticket issuer of the ticket usage condition. The ticket issuer processor closes the notification 11606 and addresses it to the ticket issuer, and transmits it as a usage report 7100 to the ticket issuing system 107.

[1665] As is shown in Fig. 116A, the digital signature of a service provider is provided for the data that consists of a usage report header 11600, which is header information indicating that the message is the usage report 7100 and describing the data structure; a ticket ID list 11601 of tickets that are employed; the merchant name 11602 and the merchant ID 11603 of a merchant that handles the ticket; a service provider ID 11604; and an issued time 11605, which indicates the date on which the usage report 7100 was issued. These data are closed and addressed to the ticket issuer, thereby providing the usage report 7100.

[1666] Upon receiving the usage report 7100, the ticket issuing system 107 decrypts it and examines the digital signature, and performs such processing as making a payment to the merchant.

[1667] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket transfer processing.

[1668] In Fig. 74 are shown procedures for the exchange of messages by the devices during the ticket transfer processing, and in Figs. 117A and 117B, 118A and 118B, and 119A and 119B are shown the contents of messages that are exchanged during the ticket transfer processing. The ticket transfer process can be performed when the ticket status 1907 of the electronic ticket indicates the transfer enabled state, which is designated by the ticket issuer when issuing a ticket.

[1669] In Fig. 74 is shown a case where user A transfers an electronic ticket to user B. The procedures for the exchange of messages by the devices belonging to users A and B are the same for infrared communication as they are for digital wireless communication. The data structures of messages are also the same.

[1670] In Fig. 74, first, when user A performs a ticket transfer process 7400, the mobile user terminal of user A transmits a ticket transfer offer 7401, which is a message offering to transfer an electronic ticket, to the mobile user terminal of user B. When at this time the mobile user terminals of user A and user B are connected, communication between user A and user B is performed via digital wireless telephone. When the mobile user terminals are not connected, infrared communication is employed.

[1671] As is shown in Fig. 117A, the digital signature of user A is provided for the data consisting of a ticket transfer offer header 11700, which is header information indicating that the message is the ticket transfer offer 7401 and describing the data structure; a transfer offer number 11701, which is an arbitrarily generated number that uniquely represents the ticket transfer process; a presentation ticket 11702 and a ticket certificate 11703 for an electronic ticket to be transferred; a ticket status 11704; variable ticket information 11705; a ticket ID 11706; an issued time 11707, which indicates the date on which the ticket transfer offer 7401 was issued; and a user public key certificate 11709. In this fashion, the ticket transfer offer 7401 is provided. The digital signature of the electronic ticket is provided, using the ticket signature private key, for the ticket status 11704, the variable ticket information 11705, the ticket ID 11706 and the issued time 11707.

[1672] The digital signature of the service provider is provided for the data that consist of a user public key header 11710; the user public key 11711 of user A; a public key certificate ID 11712, which is ID information for the public key certificate; a certificate validity term 11713; a service provider ID 11714; and a certificate issued time 11715. In this fashion, the user public key certificate 11709 is provided.

[1673] Upon receiving the ticket transfer offer 7401, the mobile user terminal of user B examines the presentation ticket 11702, the ticket certified 11703, and the digital signature of the service provider and the validity term of the public key certificate 11709. Then, the mobile user terminal examines the digital signature of the electronic ticket that is provided for the ticket status 11704, the variable ticket information 11705, the ticket ID 11706 and the issued time 11707, and the digital signature of user A accompanying the ticket transfer offer 7401, and verifies the contents of the ticket transfer offer 7401. In accordance with the presentation ticket 11702, the ticket status 11704 and the variable ticket information 11705, the mobile user terminal then displays, on the LCD, the contents of the electronic ticket that is to be transferred (display the

transfer offer; 7402).

[1674] When user B performs a transfer offer acceptance operation 7403, the mobile user terminal of user B transmits, to the mobile user terminal of user A, a ticket transfer offer response 7404, which is a response message for the ticket transfer offer 7401.

[1675] As is shown in Fig. 117B, the digital signature of user B is provided for the data that consist of a ticket transfer offer response header 11716, which is header information indicating that the message is the ticket transfer offer response 7404 and describing the data structure; an acceptance number 11717; a transfer offer number 11718; a ticket ID 11719; an issued time 11720, which indicates the date on which the ticket transfer offer response 7404 was issued; and a user public key certificate 11721. In this fashion, the ticket transfer offer response 7404 is provided.

[1676] The user public key certificate 11721 is a public key certificate for user B. To provide this certificate 11721, the digital signature of the service provider is provided for the data that consist of a user public key certificate header 11722; a user public key 11723 for user B; a public key certificate ID 11724, which is ID information for the public key certificate; a certificate validity term 11725; a service provider ID 11726; and a certificate issued time 11727.

[1677] The acceptance number 11717 is arbitrarily generated, by the mobile user terminal of user B, as a number that uniquely represents the ticket transfer processing. With this number, the mobile user terminal of user A is notified as to whether user B has accepted the ticket transfer offer 7401. When user B does not accept the ticket transfer offer 7401, a value of 0 is set as the acceptance number 11717. When user B accepts the ticket transfer offer 7401, a value other than 0 is set.

[1678] Upon receiving the ticket transfer offer response 7404, the mobile user terminal of user A displays, on the LCD, the contents of the ticket transfer offer response 7404 (display the transfer offer response; 7405). When the ticket transfer offer 7401 is accepted (acceptance number 11717 NOTEQUAL 0), the mobile user terminal of user A examines the digital signature of the service provider of the user public key certificate 11721 and the validity term. The mobile user terminal generates a ticket transfer certificate 7406, which is a message that corresponds to a transfer certificate for an electronic ticket to user B, and transmits it to the mobile user terminal of user B.

[1679] As is shown in Fig. 118A, the digital signature of the electronic ticket and the digital signature of user A are provided for the data that consist of a ticket transfer certificate header 11800, which is header information indicating that the message is the ticket transfer certificate 7406 and describing the data structure; a presentation ticket 11801 for an electronic ticket to be transferred; a ticket status 11802; variable ticket information 11803; a transfer offer number 11804; an acceptance number 11805; a public key certificate ID 11806 for the user public key certificate of user B; a public key certificate ID 11807 for the user public key certificate of user A; a ticket ID 11808; and an issued time 11809, which indicates the date on which the ticket transfer certificate 7406 was issued. These data are closed and addressed to user B, thereby providing the ticket transfer certificate 7406.

[1680] Upon receiving the ticket transfer certificate 7406, the mobile user terminal of user B decrypts it and examines the digital signature of user A and the one accompanying the electronic ticket. Further, the mobile user terminal compares the ticket ID presented by the ticket transfer offer 7401 with the ticket ID 11808, and compares the public key certificate IDs 11806 and 11807 with the public key certificates of users B and A to verify the contents of the ticket transfer certificate 7406. The mobile user terminal then generates a ticket transfer receipt 7407, which is a message indicating the electronic ticket has been received, and transmits the receipt 7407 to the mobile user terminal of user A.

[1681] As is shown in Fig. 118B, the digital signature of user B is provided for the data that consist of a ticket transfer receipt header 11815, which is header information indicating that the message is the ticket transfer receipt 7407 and describing the data structure; a ticket ID 11816; a transfer offer number 11817; an acceptance number 11818; a public key certificate ID 11819 for the user public key certificate of user A; a public key certificate ID 11820 for the user public key certificate of user B; and an issued time 11821, which indicates the date on which the ticket transfer receipt 7407 was issued. These data are closed and addressed to user A, thereby providing the ticket transfer receipt 7407.

[1682] Upon receiving the ticket transfer receipt 7407, the mobile user terminal of user A decrypts it, and examines the digital signature of user B. Further, the mobile user terminal compares the public key

certificate IDs 11819 and 11820 with the public key certificates of users B and A to verify the contents of the ticket transfer receipt 7407. The mobile user terminal then erases the transferred electronic ticket from the ticket list 1712, and registers the ticket transfer receipt 11822 in use history 1715. At this time, addresses in the object data area at which the transfer offer number, the code information indicating the ticket transfer process, the issued time for the ticket transfer receipt 7407 and the ticket transfer receipt 11822 are stored are assigned to the request number 1840 in the use list 1715, the service code 1841, the use time 1842 and the use information address 1843.

[1683] The mobile user terminal of user A displays, on the LCD, a message indicating the completion of the transfer process (display the transfer process; 7408). The process at the mobile user terminal of user A (sender) is thereafter terminated.

[1684] After transmitting the ticket transfer receipt 7407, the mobile user terminal of user B displays the received ticket transfer certificate 11811 on the LCD. In addition, the mobile user terminal displays a dialogue message inquiring whether the transfer process with the service providing server (process for downloading the received electronic ticket from the service providing system) should be immediately performed (display the transfer certificate; 7409).

[1685] The dialogue message has two operating menus: "transfer process request" and "cancel." When "cancel" is selected, the transfer process performed with the service providing server is canceled, and in the process (data updating process) during which the service providing system updates the data in the mobile user terminal, an electronic ticket that has been transferred is assigned to the mobile user terminal.

[1686] When user B selects "transfer process request" (transfer process request operation; 7410), based on the ticket transfer certificate 11811 the mobile user terminal generates a ticket transfer request 7411, which is a message requesting that the transfer process be performed with the service providing system, and transmits it to the service providing system via digital wireless telephone communication.

[1687] As is shown in Fig. 119A, the digital signature of user B is provided for the data that consists of a ticket transfer request header 11900, which is header information indicating that the message is the ticket transfer request 7411 and describing the data structure, a decrypted ticket transfer certificate 11901 (11811); the user ID 11902 of user B; and an issued time 11903, which indicates the date when the ticket transfer request 7411 was issued. These data are closed and addressed to the service provider, thereby providing the ticket transfer request 7411.

[1688] Upon receiving the ticket transfer request 7411, the user processor of user B of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the ticket transfer request 11904.

[1689] The service director processor, first refers to the user list 5200 and specifies the recipient (user B) and the sender (user A) of the transfer process by employing the public key certificate IDs 11806 and 11807 in the ticket transfer certificate 11901 that is included in the ticket transfer request 11904. The service director processor examines the digital signature of the user A and the digital signature accompanying the electronic ticket, which are provided for the ticket transfer certificate 11901, and verifies the validity of the ticket transfer certificate 11901. Following this, the service director processor exchanges the user ID 5317 for the user A with that for the user B in the user list 5301 for the electronic ticket that is stored in the service director information server 901, and erases the electronic ticket to be transferred from the ticket list of the user A that is stored in the user information server 902. Then, the service director processor changes the ticket signature private key and ticket signature public key pair and the ticket certificate for a new key pair and a ticket certificate, and also changes the ticket status and the variable ticket information to the ticket status 11802 and to the variable ticket information 11803 for the ticket transfer certificate 11901. The service director processor generates an electronic ticket received from user A, and enters it in the ticket list 4610 for the user B.

[1690] When the electronic ticket that is to be transferred has already been registered, the service director processor updates the registered ticket list 5303 holding the electronic ticket. Specifically, the user ID 5322, the user public key 5323, the registered ticket certificate address 5324, the ticket examination response list address 5325 and the former user information address 5326, all of which are in the registered ticket list 5303, are updated (to the information for user B). The old information (information for user A) is pointed to at the former user information address 5326 as former user information 5327.

[1691] The service director processor generates a ticket transfer message 11915, which includes an electronic ticket transferred from user A. The user processor of user B closes the message 11915 and addresses it to the user B, and transmits it as a ticket transfer message 7412 to the mobile user terminal of user B via digital wireless telephone communication.

[1692] As is shown in Fig. 119B, the digital signature of the service provider is provided for the data that consist of a ticket transfer header 11908, which is header information indicating that the message is the ticket transfer 7412 and describing the data structure; a transfer number 11909, which is an arbitrarily generated number that represents the transfer process in the service providing system; transfer information 11910; an acceptance number 11911; an electronic ticket 11912, which is transferred; a service provider ID 11913; and an issued time 11914, which indicates the date when the ticket transfer message 7412 was issued. These data are closed and addressed to the user B, thereby providing the ticket transfer message 7412.

[1693] The transfer information 11910 is information concerning the electronic ticket transfer process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1694] The mobile user terminal of user B decrypts the received ticket transfer message 7412 and examines the digital signature, registers the electronic ticket 11912 in the ticket list 1712, and displays the electronic ticket on the LCD (display the electronic ticket; 7413). The ticket transfer process is thereafter terminated.

[1695] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket installation processing.

[1696] In Fig. 77 are shown procedures for the exchange of messages by the devices during the ticket installation processing, and in Figs. 123A and 123B, and 124A and 124B are shown the contents of messages that are exchanged during the ticket installation processing.

[1697] First, when the user performs an electronic ticket installation operation 7700, the mobile user terminal generates an electronic ticket installation request 7701, and transmits it to the service providing system 110 via digital wireless telephone communication.

[1698] As is shown in Fig. 123A, the digital signature of the user is provided for the data that consists of an electronic ticket installation request header 12300, which is header information indicating that the message is the electronic ticket installation request 7701 and describes the data structure; an installation card number 12301 and an installation number 12302, which are entered by a user; a request number 12303, which is an arbitrarily generated number that uniquely represents the electronic ticket installation process; a user ID 12304; and an issued time 12305, which indicates the date when the electronic ticket installation request 7701 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket installation request 7701.

[1699] Upon receiving the electronic ticket installation request 7701, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the electronic ticket installation request 12306.

[1700] First, the service director processor refers to the installation card list that is indicated by the installation card list address 5229 for the ticket issuer list 5203, and specifies a ticket issuer who issues a ticket that is represented by the installation number 12301. The service director processor generates a ticket installation request 12317, which is a message requesting that the ticket issuer issue a ticket using the installation card. The ticket issuer processor closes the request 12317 and addresses it to the ticket issuer, and transmits it as a ticket installation request 7702 to the ticket issuing system 107.

[1701] As is shown in Fig. 123B, the digital signature of the service provider is provided for the data that consist of a ticket installation request header 12310, which is header information indicating that the message is the ticket installation request 7702 and describing the data structure; an installation card number 12311; an installation number 12312; a request number 12313; a customer number 12314, which uniquely represents a user for the ticket issuer; a service provider ID 12315; and an issued time 12316,

which indicates the date when the ticket installation request 7702 was issued. These data are closed and addressed to the ticket issuer, thereby providing the ticket installation request 7702.

[1702] Upon receiving the ticket installation request 7702, the ticket issuing system 107 decrypts it and examines the digital signature. The ticket issuing server 1100 compares the installation card number 12311 and the installation number 12312, which are included in the ticket installation request 7702, with the management information for the issued electronic ticket installation card that is stored in the ticket issuing information server 1102. The ticket issuing server 1100 then updates the data in the customer information server 1102 and the ticket issuing information server 1103. Furthermore, the ticket issuing server generates ticket data (12406) for a requested ticket, and transmits, to the service providing system, an electronic ticket installation commission 7703, which is a message requesting the installation of an electronic ticket that corresponds to the requested ticket.

[1703] As is shown in Fig. 124A, the digital signature of the ticket issuer is provided for the data that consists of an electronic ticket installation commission header 12400, which is header information indicating that the message is the electronic ticket installation commission 7703 and describing the data structure; a transaction number 12401, which is an arbitrarily generated number that uniquely represents the transaction with a user; ticket issuing information 12402; a request number 12403; ticket code 12404, which indicates the type of electronic ticket that is to be issued; a template code 12405, which indicates a template program for an electronic ticket to be issued; ticket data 12406; representative component information 12407; a ticket issuer ID 12408; and an issued time 12409, which indicates the date when the electronic ticket installation commission 7703 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket installation commission 7703.

[1704] The ticket issuing information 12402 is information concerning the ticket issuing process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1705] The ticket data 12406 is ticket information issued by the ticket issuer, wherein the digital signature of the ticket issuer accompanies the data that consists of the ticket ID 12414, the ticket information 12415 and the ticket ID 12416.

[1706] The ticket issuer processor of the service providing system decrypts the received electronic ticket installation commission 7703 and examines the digital signature, and transmits the commission 7703 to the service director processor. In accordance with the electronic ticket installation commission 12410, the service director processor generates an electronic ticket to be issued to a user, using the same procedures as are used for the ticket purchase processing, and also generates an electronic ticket installation message 12415, which is a message directing that the electronic ticket be installed in the mobile user terminal. The user processor closes the electronic ticket installation message 12455 and addressees it to a user, and transmits it as an electronic ticket installation message 7704 to the mobile user terminal via digital wireless telephone communication.

[1707] As is shown in Fig. 124B, the digital signature of the service provider is provided for the data that consists of an electronic ticket installation header 12417, which is header information indicating that the message is the electronic ticket installation message 7704 and describing the data structure; a transaction number 12418; ticket issuing information 12419, which concerns the ticket issuing process performed by the ticket issuing system; ticket issuing information 12420, which concerns the ticket issuing process performed by the service providing system; a request number 12421; generated electronic ticket code 12422; a service provider ID 12423; and an issued time 12424, which indicates the date when the electronic ticket installation message 7704 was issued. These data are closed and addressed to the user, thereby providing the electronic ticket installation message 7704. The ticket issuing information 12419 and the ticket issuing information 12420 are accompanied by the digital signatures of the ticket issuer and the service provider.

[1708] The mobile user terminal decrypts the received electronic ticket installation message 7704 and examines the digital signature, registers, in the ticket list 1712, the electronic ticket included in the electronic ticket installation request 7704, and displays the installed electronic ticket on the LCD (display the electronic ticket; 7705).

[1709] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket modification processing.

[1710] In Fig. 80 are shown procedures for the exchange of messages by the gate terminal 101, the service providing system 110 and the ticket issuing system 107 during the processing performed to modify the ticket examination program of the gate terminal. In Figs. 129A and Figs. 88C, 88D and 88F are shown the contents of messages that are exchanged by the gate terminal 101, the service providing system 110 and the ticket issuing system 107 during the ticket modification processing. In Fig. 81 are shown procedures for the exchange of messages by the mobile user terminal 100, the service providing system 110 and the ticket issuing system 107 during the processing performed to modify the electronic ticket of the mobile user terminal. In Figs. 129A and 129B, and Figs. 130A and 130B are shown the contents of messages that are exchanged by the mobile user terminal 100, the service providing system 110 and the ticket issuing system 107.

[1711] When the contents of a ticket that was issued must be altered because an event was changed or an error was found when the ticket was issued, the ticket issuing system generates a modification request 8000 or 8100, which is a message requesting the modification of a ticket that was issued, and transmits it to the service providing system.

[1712] As is shown in Fig. 129A, the digital signature of the ticket issuer is provided for the data that consist of a modification request header 12900, which is header information indicating that the message is the modification request 8000 or 8100 and describing the data structure; a modification number 12901, which is an arbitrarily generated number that uniquely represents the ticket modification processing; a modification code 12902; a modification time limit 12903, which indicates the time limit for the modification; a modification message 12904; a ticket code 12905, which indicates the type of electronic ticket that is to be modified; a template code 12906, which identifies a template program for a modified electronic ticket; a ticket count 12907 that indicates the number of electronic tickets to be modified; modified ticket data 12908; modified representative component information 12909; a ticket issuer ID 12910; and an issued time 12911, which indicates the date when the ticket modification request 8000 was issued. These data are closed and addressed to the service provider, thereby providing the ticket modification request 8000 or 8100.

[1713] The modification code 12902 is code information that identifies the type of ticket modification processing, and that indicates the modification of the electronic ticket information 1917, the modification of the representative component information 1932, the modification of the template program, or the modification accompanied by the ticket refund processing will be performed.

[1714] The modification message 12904 specifies the contents of the modification, and is accompanied by the digital signature of the ticket issuer.

[1715] The ticket data 12908 is modified ticket information for an electronic ticket to be modified. Tickets in a number equivalent to the ticket count 12907 are set as ticket data 12908. The ticket information is obtained by providing the digital signature of the ticket issuer for the data that consists of the ticket ID 12916, the ticket information 12917 and the ticket issuer ID 12918. When no modification of the electronic ticket information is to take place, the ticket data 12908 are not set.

[1716] The representative component information 10209 is set as the modified representative component information 1932 for an electronic ticket that is to be modified. When no modification is scheduled for the representative component information 1932, the representative component information 10209 is not set.

[1717] The ticket issuer processor of the service providing system 110 decrypts the received modification request 8000 or 8100 and examines the digital signature, and transmits the request to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the modification request 12912. Then, the service director processor changes the electronic ticket of the mobile user terminal and the ticket examination program of the gate terminal in accordance with the modification request 12912. The ticket examination program for the gate terminal is changed when the template program is modified.

[1718] An explanation will now be given for the processing performed to change the ticket examination program for the gate terminal.

[1719] First, the service director processor generates a new ticket examination program by employing the ticket examination module, which is pointed to at the ticket examination module address 4922 in the electronic ticket template list 4905 indicated by the template code 12906, and the ticket public key 5309 and the gate private key 5310, which are registered in the electronic ticket management information 5300.

Then, the service director processor refers to the examination ticket list 4711 for the gate terminal of the merchant who is registered in the merchant list 5302 to obtain the electronic ticket that is to be modified, and specifies that the gate terminal for which the electronic ticket to be modified is registered is an electronic ticket that the gate terminal is to examine. The service director processor transmits, to the merchant processor of the gate terminal that is specified, a message requesting the performance of the forcible data updating process to update the ticket examination program.

[1720] The merchant processor of the specified gate terminal performs the forcible data updating process, and modifies the ticket examination program of the gate terminal. At this time, the procedures for the exchange of messages by the gate terminal and the service providing system, and the contents (data structures) of the messages that are exchanged are the same as those employed for the forcible data updating processing that was previously described.

[1721] The merchant processor inserts the new ticket examination program into the compressed update data 8828 of the update data 5708, and transmits the resultant data to the gate terminal as the update data 5708.

[1722] Upon receiving the update data 5708, the gate terminal decompresses the update data 8828, and updates the data in the RAM and on the hard disk. At this time, the ticket examination program is also registered in the ticket list 2409 of the gate terminal.

[1723] An explanation will now be given for the processing for modifying an electronic ticket in the mobile user terminal. First, the service director processor refers to the user list 5301 for an electronic ticket to be modified, and specifies a user who owns the electronic ticket that is to be modified. The service director processor generates a modification notification 12928, which is a message for notifying the specified user of the modification of the electronic ticket. The user processor for the specified user closes the modification notification 12928, addresses it to the user, and transmits it as a modification notification 8101 to the mobile user terminal via digital wireless telephone communication.

[1724] As is shown in Fig. 129B, the digital signature of the service provider is provided for the data that consist of a modification notification header 12920, which is header information indicating that the message is the modification notice 8101 and describing the data structure; a modification number 12921; a modification code 12922; a ticket ID 12923; a modification message 12924; a reply time limit 12925, which specifies the time limit for the transmission of a replay (reaction selection 8104) by the user to the modification notice 8101; a service provider ID 12926; and an issued time 12927, which indicates the date on which the modification notice 8101 was issued. These data are closed and addressed to the user, thereby providing the modification notice 8101.

[1725] Upon receiving the modification notice 8101, the mobile user terminal decrypts it and examines the digital signature, outputs a call arrival tone to notify the user of the reception of the modification notice 8101, and displays a modification message 12924 on the LCD (display the modification notice; 8102). For example, when the date has been changed, a message to that effect and a message requesting that the user select an action, either "accept," "refuse" or "refund," in response to the modification are displayed.

[1726] When, in response to the message displayed on the LCD, the user employs the number key switches to select an action in response to the modification (reaction selection operation 8103), the mobile user terminal generates a reaction selection message 8104, which contains the response of the user to the modification notice 8101, and transmits it to the service providing system via the digital wireless telephone communication. When the user selects "refuse" or "refund," the mobile user terminal changes the ticket status 1907 of the electronic ticket to the use disabled state.

[1727] As is shown in Fig. 130B, the digital signature of the user is provided for the data that consists of a reaction selection header 13000, which is header information indicating that the message is the reaction selection message 8104 and describing the data structure; a modification number 13001; a reaction code 13002, which identifies the type of reaction to the modification that the user selected; a ticket ID 13004, which is a number that is arbitrarily generated, by the mobile user terminal, that uniquely represents the ticket modification; a user ID 13005; and an issued time 13006, which indicates the date on which the selection message 8104 was issued. These data are closed and addressed to the service provider, thereby providing the reaction selection message 8104.

[1728] The user processor of the service providing system decrypts the received reaction selection

message 8104, examines the digital signature, and transmits it to the service director processor. The service director processor updates the contents of an electronic ticket, or refunds the cost of the ticket in accordance with the reaction code 13002 contained in the reaction selection message 13007. When the user selects "refuse," the service director processor changes to the use disabled state the ticket status 4647 of the corresponding electronic ticket in the ticket list 4610 for the user, which is stored in the user information server 902.

[1729] When the reaction code 13002 represents "accept," in response to the modification request 8100, the service director processor generates a new electronic ticket using the same procedures as those used during the ticket purchase processing. In addition, the service director processor generates a modification instruction 13017, which is a message for instructing the modification of a ticket, and transmits it to the user processor. The user processor changes a corresponding electronic ticket in the user ticket list 4610 to an electronic ticket that is included in the modification instruction 13017. The user processor closes the modification instruction 13017 and addresses it to the user, and transmits it as a modification instruction 8105 to the mobile user terminal via digital wireless telephone communication.

[1730] As is shown in Fig. 130A, the digital signature of the service provider is provided for the data that consists of a modification reaction header 13011, which is header information indicating that the message is the modification instruction 8105 and describing the data structure; a modification number 13012; a request number 13013; new electronic ticket data 13014; a service provider ID 13015; and an issued time 13016, which indicates the date on which the modification instruction 8105 was issued. These data are closed and addressed to the user, thereby providing the modification instruction 8105.

[1731] Upon receiving the modification instruction 8105, the mobile user terminal decrypts it and examines the digital signature. Then, instead of the old electronic ticket, the mobile user terminal registers in the ticket list 1712 the new electronic ticket 13014 that is included in the modification instruction 8105, and displays the new electronic ticket on the LCD (display the ticket; 8106).

[1732] An explanation will now be given for the contents of the messages that are exchanged by the devices during the ticket refund processing.

[1733] In Fig. 82 are shown procedures for exchanging messages when the ticket refund processing is performed by immediate clearing. In Figs. 131A and 131B, 133A and 133B, and 134A and 134B are shown the contents of messages that are exchanged by the devices during the ticket refund processing. In Fig. 83 are shown procedures for exchanging messages when the ticket refund processing is performed by delayed clearing. In Figs. 131A and 131B, 132A and 132B, 133A and 133B, and 134A and 134B are shown the contents of messages that are exchanged by the devices.

[1734] The ticket refund process is performed when the user selects "refund" during in the ticket modification process (when the reaction code 13002 of the reaction selection message 13007 represents "refund"). Therefore, the message exchanging procedures up to the reaction selection 13007 are transmitted by the user processor to the service director processor, and the contents of those messages are the same as those employed for the ticket modification processing.

[1735] When the reaction code 13002 indicates "refund," the service director processor generates a refund request 13107, which is a message requesting that the ticket issuer refund the cost of the ticket. The ticket issuer processor closes the request 13107, addressing it to the ticket issuer, and transmits it as a refund request 8205 or 8305 to the ticket issuing system.

[1736] As is shown in Fig. 131A, the digital signature of the service provider is provided for the data that consist of a refund request header 13100, which is header information indicating that the message is a refund request and describing the data structure; a modification number 13101; a ticket ID 13102 for a ticket for which the cost is to be refunded; a request number 13103; a customer number 13104; a service provider ID 13105; and an issued time 13106, which indicates the date on which the refund request was issued. These data are closed and addressed to the ticket issuer, thereby providing the refund request 8205 or 8305.

[1737] Upon receiving the refund request 8205 or 8305, the ticket issuing server 1100 of the ticket issuing system updates data in the customer information server 1101, the ticket issuing information server 1102 and the ticket information server 1103, cancels the issued ticket, generates a refund commission 8206, which is a message requesting that the service providing system perform the refund process for an

electronic ticket, and transmits the commission 8206 to the service providing system.

[1738] As is shown in Fig. 131B, the digital signature of the ticket issuer is provided for the data that consists of a refund commission header 13111, which is header information indicating that the message is the refund commission and describing the data structure; a transaction number 13112, which is an arbitrarily generated number that uniquely represents the ticket refund processing; a refund amount 13113; a clearing option 13114; a ticket ID 13115; a request number 13116; a ticket issuer ID 13117; and an issued time 13118, which indicates the date when the refund commission was issued. These data are closed and addressed to the service provider, thereby providing the refund commission 8206 or 8306.

[1739] The ticket issuer processor of the service providing system decrypts the received refund commission 8206 or 8306 and examines the digital signature, and transmits it to the service director processor. When the clearing option 13114 in the refund commission 13119 represents immediate clearing, the service director processor performs the refund process using immediate clearing. When the clearing option 13114 represents delayed clearing, the service director processor performs the ticket refund process using delayed clearing.

[1740] An explanation will now be given for the ticket refund process that uses immediate clearing.

[1741] In Fig. 82, upon receiving a refund commission 13119, the service director processor generates a refund clearing request 13222, which is a message requesting the performance of the refund clearing process. The transaction processor processor closes the request 13222 and addresses it to the transaction processor, and transmits it as a refund clearing request 8207 to the transaction processing system 106.

[1742] As is shown in Fig. 132B, the digital signature of the service provider is provided for the data that consists of a refund clearing request header 13212, which is header information indicating that the message is the refund clearing request 8207 and describing the data structure; a user clearing account 13213; a ticket issuer clearing account 13214, which indicates the clearing account of the ticket issuer; a refund amount 13215; a refund option code 13216; a request number 13217, which is issued by the mobile user terminal 100; a transaction number 13218, which is issued by the ticket issuing system; a validity term 13219, which specifies a period during which the refund clearing request 5904 is valid; a service provider ID 13220; and an issued time 13221, which indicates the date when the refund clearing request 5904 was issued. These data are closed and addressed to the transaction processor, thereby providing the refund clearing request 8207.

[1743] Upon receiving the refund clearing request 8207, the transaction server 1000 of the transaction processing system updates data in the subscriber information server 1001, the member store information server 102 and the transaction information server 103, performs the refund clearing process, and generates for the service providing system a refund clearing completion notification 8208 that is a message indicating that the refund clearing has been completed.

[1744] As is shown in Fig. 133A, the digital signature of the transaction processor is provided for the data that consists of a refund clearing completion notification header 13300, which is header information indicating that the message is the refund clearing notification 8208 and describing the data structure; a clearing number 13301, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 13302; a ticket issuer clearing account 13303; a refund amount 13304; a refund option code 13305; a request number 13306; a transaction number 13307; clearing information 13308 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 13309 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 13311; and an issued time 13312, which indicates the date when the refund clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the refund clearing completion notification 8208.

[1745] The transaction processor processor of the service providing system 110 decrypts the received refund clearing completion notification 8208 and examines the digital signature, and transmits the refund clearing completion notification 13313 to the service director processor. The service director processor employs the refund clearing completion notification 13313 to generate a refund clearing completion notification 13329 for the ticket issuer. The ticket issuer processor closes the notification 13329, addresses it to the ticket issuer, and transmits it as a refund clearing completion notification 8209 to the ticket issuing system 107.

[1746] As is shown in Fig. 133B, the digital signature of the service provider is provided for the data that consist of a refund clearing completion notification header 13317, which is header information indicating that the message is the refund clearing notification 8209 and describing the data structure; a clearing number 13318; a customer number 13319; a ticket issuer ID 13320; a refund amount 13321; a clearing option 13322; a request number 13323; a transaction number 13324; clearing information 13325 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 13326; a service provider ID 13327; and an issued time 13328, which indicates the date when the refund clearing completion notification was issued. These data are closed and addressed to the ticket issuer, thereby providing the refund clearing completion notification 8209.

[1747] The ticket issuing system decrypts the received refund clearing completion notification 8209 and examines the digital signature, generates a refund receipt 8210, and transmits it to the service providing system.

[1748] As is shown in Fig. 134A, the digital signature of the ticket issuer is provided for the data that consists of a refund receipt header 13400, which is header information indicating that the message is the refund receipt 8210 and describing the data structure; a customer number 13201; refund information 13402; a refund amount 13403; a request number 13404; a transaction number 13405; a clearing number 13406;a transaction processor ID 13407; a ticket issuer ID 13408; and an issued time 13409, which indicates the date when the refund receipt 8210 was issued. These data are closed and addressed to the service provider, thereby providing the refund receipt 8210. The refund information 13402 concerns the refund process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1749] The ticket issuer processor of the service providing system 110 decrypts the received refund receipt 8210 and examines the digital signature, and transmits the refund receipt 13410 to the service director processor. The service director processor employs the refund receipt 13410 to generate a refund receipt 13421 to be transmitted to the user.

[1750] When the service director processor has transmitted the refund clearing completion notification 13329 to the ticket issuing system, the service director processor erases from the user ticket list 4610 stored in the user information server 902 the electronic ticket for which the refund was effected.

[1751] The user processor closes the refund receipt 13421, addressing it to the user, and transmits it as a refund receipt 8211 to the mobile user terminal 100 via digital wireless telephone communication.

*[1752] As is shown in Fig. 134B, the digital signature of the service provider is provided for the data that consists of a refund receipt header 13414, which is header information indicating that the message is the refund receipt 8211 and describing the data structure; a user ID 13415; a decrypted refund receipt 13416 (13410); clearing information 13417 for a user that is accompanied by the digital signature of the transaction processor; refund information 13418; a service provider ID 13419; and an issued time 13420, which indicates the date when the refund receipt 8211 was issued. These data are closed and addressed to the user, thereby providing the refund receipt 8211. The refund information 13418 concerns the electronic ticket refund process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1753] The mobile user terminal decrypts the received refund receipt 8211 and examines the digital signature, erases from the check list 1712 the electronic ticket for which the refund was effected, registers the refund receipt 13421 in the use list 1715, and displays the refund receipt 13421 on the LCD 303 (display the refund receipt; 8212).

[1754] An explanation will now be given for the ticket refund processing performed with the delayed clearing. In Fig. 83, the procedures up to the time the ticket issuing system transmits a refund commission to the service providing system are the same as are those for the immediate clearing.

[1755] When the delayed clearing is designated in accordance with the clearing option 13114, the service director processor generates a temporary refund receipt 13208 that corresponds to a temporary receipt for the refund process. The user processor closes the temporary refund receipt 13208, addressing it to the user, and transmits it as a temporary refund receipt 8307 to the mobile user terminal 100 via digital wireless

telephone communication.

[1756] As is shown in Fig. 132A, the digital signature of the service provider is provided for the data that consist of a temporary refund receipt header 13200, which is header information indicating that the message is the temporary refund receipt 8307 and describe the data structure; a user ID 13201; refund information 13202; a refund amount 13203; a request number 13204; a transaction number 13205; a service provider ID 13206; and an issued time 13207, which indicates the date when the temporary refund receipt 8307 was issued. These data are closed and addressed to the user, thereby providing the temporary refund receipt 8307. The refund information 13202 concerns the electronic ticket refund process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1757] The mobile user terminal decrypts the received temporary refund receipt 8307 and examines the digital signature, erases the electronic ticket that is refund from the check list 1712, registers the temporary refund receipt 13208 to the use list 1715, and displays the temporary refund receipt 13208 on the LCD 303 (display the refund receipt; 8308).

[1758] The service director processor thereafter performs the refund clearing processing.

[1759] First, the service director processor generates the refund clearing request 13222, which is a message requesting the performance of the refund clearing process. The transaction processor processor closes the request 13222, addressing it to the transaction processor, and transmits it as a refund clearing request 8309 to the transaction processing system 106.

[1760] The transaction processing system 106 decrypts the received refund clearing request 8309 and examines the digital signature, and performs the refund clearing process. Then, the transaction processing system 106 generates a refund clearing completion notification 8310, and transmits it to the service providing system 110.

[1761] The transaction processor processor of the service providing system 110 decrypts the received refund clearing completion notification 8310 and examines the digital signature, and transmits a refund clearing completion notification 13313 to the service director processor. The service director processor employs the refund clearing completion notification 13313 to generate the refund clearing completion notification 13329 for the ticket issuer. The ticket issuer processor closes the notification 13329, addressing it to the ticket issuer, and transmits it to the ticket issuing system 107 as a refund clearing completion notification 8311 for the ticket issuer.

[1762] The ticket issuing system decrypts the received refund clearing completion notification 8311 and examines the digital signature, and generates a refund receipt 8312 and transmits it to the service providing system.

[1763] The ticket issuer processor of the service providing system 110 decrypts the received refund receipt 8312 and examines the digital signature, and transmits a refund receipt 13410 to the service director processor. The service director processor employs the refund receipt 13410 to generate a refund receipt 13412 for the user.

[1764] The generated refund receipt 13412 is not immediately transmitted to the mobile user terminal 100 of the user, but when the mobile user terminal 100 performs the data updating process, the user processor replaces the temporary refund receipt 13208 in the use list 1715 with the refund receipt 13421, and transmits it as a part of the update data 8313 to the mobile user terminal 100.

[1765] The data structures of the refund clearing request 8309, the refund clearing completion notification 8310, the refund clearing completion notification 8311 and the refund receipt 8312 for the delayed clearing are the same as those used for the refund clearing request 8207, the refund clearing completion notification 8208, the refund clearing completion notification 8209 and the refund receipt 8210 for the immediate clearing.

[1766] The refund clearing process with the delayed clearing is not necessarily performed immediately after the temporary refund receipt is issued, and may be performed, for example, once a day with another clearing process.

[1767] An explanation will now be given for the contents of messages that are exchanged by devices in various processes for electronic payment card service.

[1768] First, an explanation will be given for the contents of messages that are exchanged by devices during the payment card purchase processing.

[1769] In Fig. 61 are shown the procedures for the exchange of messages by devices during the payment card purchase processing. In Figs. 96A and 96B, 97A and 97B, 98A and 98B, 99A and 99B, and 100A and 100B are shown the contents of messages that are exchanged by devices during the payment card purchase processing.

[1770] First, when a user performs a payment card purchase order operation 6100, the mobile user terminal transmits a payment card purchase order 6101 to the service providing system through digital wireless telephone communication.

[1771] As is shown in Fig. 96A, the digital signature of a user is provided for data that consists of a payment card purchase order header 9600, which is header information identifying the message as the payment card purchase order 6101 and describing the data structure; a response code 9601, which identifies the type of service requested by the user; a card order code 9602, which identifies an order code for a payment card that is entered by the user; a number of payment cards 9603 that the user has entered; a payment service code 9604, which identifies a credit card designated by the user; a payment value 9605; a payment option code 9606, which identifies a payment option, such as the number of payments designated by the user; a request number 9607, which is an arbitrarily generated number that uniquely represents the payment card purchase processing; a validity term 9608 for the payment card purchase order 6101; a user ID 9609; and an issued time 9610, which is the date on which the payment card purchase order 6101 was issued. These data are closed and addressed to the service provider, thereby providing the payment card purchase order 6101. The service code 8901 identifies the purchase order of a payment card to a payment card issuer who is selected by the user.

[1772] Upon receiving the payment card purchase order 6101, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group that processes a payment card order 9611. The service director processor refers to the payment card issuer list 5204 and generates a payment card purchase order 9626 for the payment card issuer indicated by the service code 9601. The payment card issuer processor closes the payment card order and addresses it to the payment card issuer, and transmits the resultant order as a payment card purchase order 6102 to the payment card issuing system 108.

[1773] As is shown in Fig. 96B, the digital signature of a service providing system is provided for data that consists of a payment card purchase order header 9615, which is header information indicating that the message is the payment card purchase order 6102 and describing the data structure; a card order code 9616; a number of cards 9617 that are purchased; a payment service code 9618; a payment value 9619; a payment option code 9620; a request number 9621; a customer number 9622, which uniquely represents a user for the payment card issuer; a validity term 9623 for the payment card purchase order 6102; a service provider ID 9624; and an issued time 9625, which is the date on which the payment card purchase order 6102 was issued. These data are closed and addressed to the payment card issuer, thereby providing the payment card purchase order 6102.

[1774] When there was a previous transaction to which the user and the payment card issuer were parties, a customer number that is registered in the customer table of the payment card issuer is established as the customer number 9622. When there was no previous transaction, the service director processor generates for the payment card issuer a number that uniquely represents the user, establishes it as the customer number 9622, and registers that number in the customer table. The customer table is designated by using the customer table address 5237 of the payment card issuer list 5204.

[1775] Upon receiving the payment card purchase order 6102, the payment card issuing system 108 decrypts it and examines the digital signature. The payment card issuing server 1200 updates the data in the customer information server 1201, the payment card issuing information server 1202 and the payment card information server 1203, generates payment card data (9719) for the ordered payment card, and transmits, to the service providing system, an electronic payment card issuing commission 6103, which constitutes a message requesting the process for issuing an electronic payment card that corresponds to

the payment card and the process for settling the price of the payment card.

[1776] As is shown in Fig. 97A, the digital signature of a payment card issuer is provided for data that consists of an electronic payment card issuing commission header 9700, which is header information identifying the message as the electronic payment card issuing commission 6103 and describing the data structure; a transaction number 9701, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 9702, which conveys the price of a payment card; a clearing option 9703, which indicates which clearing procedures apply; a request number 9704; a payment card code 9705, which identifies the type of electronic payment card that is to be issued; a template code 9706, which identifies a template program to be used for an electronic payment card that is to be issued; a number of payment cards 9707, which indicates how many payment cards are to be issued; payment card data 9708; representative component information 9709; a payment card issuer ID 9710; and an issued time 9711, which is the date on which the electronic payment card issuing commission 6103 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card issuing commission 6103.

[1777] The clearing option 9703 is information by which the payment card issuing system designates, to the service providing system, the procedures to be used for clearing the price of a payment card. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic payment card to a user after the price of the payment card has been cleared, and a delayed clearing process for clearing the price of a payment card after an electronic payment card has been issued. The clearing option 9703 is used to designate either clearing process.

[1778] In the delayed clearing process, since an electronic payment card is issued to a user before the clearing process is performed, the user does not have to wait.

[1779] For example, based on a purchase history maintained for customers, the payment card issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known to be trustworthy, and can designate the spontaneous clearing for a customer with whom it has had no previous dealings.

[1780] The payment card data 9708 is payment card information issued by the payment card issuer. A number of payment card information items equivalent to the number of payment cards 9707 are established as the payment card data 9708. For one payment card, the digital signature of a payment card issuer is provided for data that consist of a card ID 9716, card information 9717 and a payment card issuer ID 9718, and the payment card information is thereby provided. The payment card information 9717 is ASCII information describing the contents of a payment card. For the payment card information 9717, the title of a payment card, the face value of the payment card that is issued, the usage condition, an issuer, and whether it can be transferred, are described using a form whereby tag information representing information types is additionally provided.

[1781] The representative component information 9709 is information that is established as the representative component information 2032 for an electronic payment card to be generated. Therefore, the representative component information 9709 may not be set for use.

[1782] The payment card issuer processor of the service providing system receives the electronic payment card issuing commission 6103, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic payment card issuing process and the payment card price clearing process in accordance with the clearing procedures designated by using the clearing option 9703.

[1783] In Fig. 61 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1784] For the spontaneous clearing, the service director processor generates a clearing request 9824, which is a message requesting the clearing of the price of a payment card. The transaction processor processor closes the clearing request 9824 and addresses it to the transaction processor, and then transmits it as a clearing request 6104 to the transaction processing system 106.

[1785] As is shown in Fig. 98B, the digital signature of a service provider is provided for data that consists of a clearing request header 9814, which is header information indicating that the message is the clearing

request 6104 and describing the data structure; a user clearing account 9815, which includes a credit card that corresponds to the payment service code designated by the user; a payment card issuer clearing account 9816, which designates the clearing account of a payment card issuer; a payment value 9817; a payment option code 9818; a request number 9819, which is issued by the mobile user terminal 100; a transaction number 9820, which is issued by the payment card issuing system; a validity term 9821, which presents the period during which the clearing request 6104 is effective; a service provider ID 9822; and an issued time 9823, which indicates the date on which the clearing request 6104 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 6104.

[1786] The transaction processing system 106 receives the clearing request 6104, decrypts it and examines the digital signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 6105, and transmits it to the service providing system 110.

[1787] As is shown in Fig. 99A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 9900, which is header information indicating that the message is the clearing completion notification 6105 and describing the data structure; a clearing number 9901, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 9902; a payment card issuer clearing account 9903; a payment value 9904; a payment option code 9905; a request number 9906; a transaction number 9907; clearing information 9908 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 9909 for a payment card issuer that is accompanied by the digital signature of the transaction processor; clearing information 9910 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 9911; and an issued time 9912, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 6105.

[1788] Upon receiving the clearing completion notification 6105, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9913 to the service director processor. Upon receiving the clearing completion notification 9913, the service director processor generates a clearing completion notification 9930 for the payment card issuer. The payment card issuer processor closes the clearing completion notification 9930, and transmits it to the payment card issuing system 107 as a clearing completion notification 6106 for the payment card issuer.

[1789] As is shown in Fig. 99B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 9917, which is header information indicating that the message is the clearing completion notification 6106 and describing the data structure; a clearing number 9918; a customer number 9919; a payment card issuer ID 9920; a payment service code 9921; a payment value 9922; a payment option code 9923; a request number 9924; a transaction number 9925; clearing information 9926 for a payment card issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 9927; a service provider ID 9928; and an issued time 9929, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the payment card issuer, thereby providing the clearing completion notification 6106.

[1790] Upon receiving the clearing completion notification 6106, the payment card issuing system decrypts it and examines the digital signature, and generates a receipt 6107 and transmits it to the service providing system.

[1791] As is shown in Fig. 100A, the digital signature of a payment card issuer is provided for data that consists of a receipt header 10000, which is header information indicating that the message is the receipt 6107 and describing the data structure; a customer number 10001; payment card issuing information 10002; a payment service code 10003; a payment value 10004; a payment option code 10005; a request number 10006; a transaction number 10007; clearing information 10008; a transaction processor ID 10009; a payment card issuer ID 10010; and an issued time 10011, which indicates the date on which the receipt 6107 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 6107. The payment card issuing information 10002 is information concerning the payment card issuing process performed by the payment card issuing system, and is accompanied by the digital signature of the payment card issuer.

[1792] Upon receiving the receipt 6107, the payment card issuer processor of the service providing system

110 decrypts it and examines the digital signature, and transmits a receipt 10012 to the service director processor. The service director processor employs the receipt 10012 to generate a receipt 10023 for a user.

[1793] In addition, the service director processor generates a clearing completion notification 9930 for the payment card issuing system, generates an electronic payment card to be issued to the user, and further generates an electronic payment card issuing message 9227 that includes the electronic payment card that is generated.

[1794] The user processor closes the electronic payment card issuing message 9227 and the receipt 10023 while addressing them to the user, and transmits them as an electronic payment card issuing message 6108 and a receipt 6109 to the mobile user terminal 100 via digital wireless communication.

[1795] As is shown in Fig. 97B, the digital signature of a service provider is provided for data that consist of an electronic payment card issuing header 9720, which is header information indicating that the message is the electronic payment card issuing message 6108 and describing the data structure; a transaction number 9721; a request number 9722; the number of payment cards 9723; electronic payment card data 9724 that are generated; a service provider ID 9725; and an issued time 9726, which indicates the date on which the electronic payment card issuing message 6108 was issued. These data are closed and addressed to the user, thereby providing the electronic payment card issuing message 6108. The electronic payment card data 9724 includes electronic payment cards 9731 equivalent in number to the number of payment cards 9723.

[1796] As is shown in Fig. 100B, the digital signature of a service provider is provided for data that consists of a receipt header 10016, which is header information indicating that the message is the receipt 6109 and describing the data structure; a user ID 10017; a receipt 10018 (10012) obtained by decryption; clearing information 10019 for a user that is accompanied by the digital signature of a transaction processor; payment card issuing information 10020; a service provider ID 10021; and an issued time 10022, which indicates the date on which the receipt 6109 was issued. These data are closed and addressed to the user, thereby providing the receipt 6109. The payment card issuing information 10020 is information for the electronic payment card issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1797] Upon receiving the electronic payment card issuing message 6108 and the receipt 6109, the mobile user terminal decrypts them and examines the digital signatures, enters in the payment card list 1713 an electronic payment card included in the electronic payment card issuing message 6108, enters the receipt 10023 in the use list 1715, and displays the electronic payment card on the LCD 303.

[1798] The generation of an electronic payment card by the service director processor is performed as follows.

[1799] First, the service director processor refers to the electronic payment card template list 5005 for the payment card issuer that is stored in the payment card issuer information server. Then, by using the electronic payment card template program that is identified by the template code 9706 of the electronic payment card issuing commission 6103, the service director processor generates a payment card program for an electronic payment card. Specifically, the payment card program data 2013 for an electronic payment card are generated using the transaction module and the representation module, which are described as being located at the transaction module address 5019, and the representation module address 5020 in the electronic payment card template list 5005, and the representative component information 9709 in the electronic payment card issuing commission 6103. When the representative component information 9709 is not present in the electronic payment card issuing commission 6103, the default representative component information located at the default representative component information address 5021 is employed as the information for an electronic payment card.

[1800] Following this and based on the payment card information included in the card information 9717, the service director processor generates the card status 2007 and the total remaining value 2008. Whether the card status 2007 can be transferred is designated, and the face value of the payment card that is issued is set as the total remaining value 2007. The service director processor generates a new pair consisting of a card signature private key and a card signature public key, and further generates the payment card program 2001 for an electronic payment card by employing the card private key and the accounting machine public key that are registered in the electronic payment card management information 5400.

[1801] Furthermore, the service director processor generates an electronic payment card by employing the obtained card signature public key to generate the certificate 2003 for the electronic payment card, and by employing the payment card data 9719 in the electronic payment card issuing commission 6103 to generate the presentation card 2002 for the electronic payment card.

[1802] The procedures for the delayed clearing will now be described.

[1803] In Fig. 62 are shown the procedures for exchanging messages between the devices in the payment card purchase process for the delayed clearing. The same process is performed as is used for the spontaneous clearing until the payment card issuing system transmits the electronic payment card issuing commission to the service providing system.

[1804] When the delayed clearing is designated by the clearing option 9703, the service director processor generates an electronic payment card to be issued to the user, and also generates the electronic payment card issuing message 9727, which includes the generated electronic payment card, and a temporary receipt message 9810, which corresponds to a temporary receipt. The generation of the electronic payment card is performed in the same manner as that used for the spontaneous clearing.

[1805] The user processor closes the electronic payment card issuing message 9727 and the temporary receipt 9810 and addresses them to the user, and transmits these messages as an electronic payment card issuing message 6204 and a temporary receipt 6205 to the mobile user terminal 100 via digital wireless telephone communication.

[1806] As is shown in Fig. 98A, the digital signature of a service provider is provided for data that consists of a temporary receipt header 9800, which is header information indicating that the message is the temporary receipt 6205 and describing the data structure; a user ID 9801; payment card issuing information 9802; a payment service code 9803; a payment value 9804; a payment option code 9805; a request number 9806; a transaction number 9807; a service provider ID 9808; and an issued time 9809, which indicates the date on which the temporary receipt 6205 was issued. These data are closed and addressed to the user, thereby providing the temporary receipt 6205. The payment card issuing information 9802 is information concerning the electronic payment card issuing process that is performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1807] The data structure of the electronic payment card issuing message 6204 is the same as that used for the electronic payment card issuing message 6108.

[1808] Upon receiving the electronic payment card issuing message 6204 and the temporary receipt 6205, the mobile user terminal decrypts them and examines the digital signatures, enters an electronic payment card included in the electronic payment card issuing message 6204 in the payment card list 1713, enters the temporary receipt 9810 in the use list 1715, and displays the electronic payment card on the LCD 303.

[1809] Following this, the service director processor performs the clearing process for the price of the payment card. First, the service director processor generates a clearing request 9824, which is a message requesting the performance of the clearing process for the price of the payment card. The transaction processor closes the clearing request 9824 and addresses it to the transaction processor, and transmits it as a clearing request 6207 to the transaction processing system 106.

[1810] Upon receiving the clearing request 6207, the transaction processing system 106 decrypts it and examines the digital signature, and performs the clearing process. The transaction processing system 106 generates a clearing completion notification 6208 and transmits it to the service providing system 110.

[1811] Upon receiving the clearing completion notification 6208, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9913 to the service director processor. The service director processor employs the received clearing completion notification 9913 to generate a clearing completion notification 9930 for the payment card issuer. And the payment card issuer processor closes the clearing completion notification 9930 and transmits it to the payment card issuing system 108 as a clearing completion notification 6209 for the payment card issuer.

[1812] The payment card issuing system decrypts the received clearing completion notification 6209 and

examines the digital signature, and generates a receipt 6210 and transmits it to the service providing system.

[1813] The payment card issuer processor of the service providing system decrypts the received receipt 6210 and examines the digital signature, and transmits a receipt 10012 to the service director processor. The service director processor employs the receipt 10012 to generate a receipt 10023 for a user.

[1814] The receipt 10023 that is generated is not immediately transmitted to the mobile user terminal 100 of the user. When the mobile user terminal has performed the data updating process, the user processor replaces the temporary receipt 9810 in the use list 1715 with the receipt 10023, and transmits the receipt 10023 as one part of the update data 6211 to the mobile user terminal 100.

[1815] The data structures of the clearing request 6207, the clearing completion notification 6208, the clearing completion notification 6209 and the receipt 6210 for the delayed clearing are the same as those provided for the clearing request 6104, the clearing completion notification 6105, the clearing completion notification 6106 and the receipt 6107 for the spontaneous clearing.

[1816] The delayed clearing process need not be performed immediately after the electronic payment card is issued, and together with the other clearing processes, may be performed, for example, once a day.

[1817] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110 during the payment card registration processing.

[1818] In Fig. 65B are shown the procedures for exchanging messages between devices in the payment card registration processing, and in Figs. 107A and 107B are shown the contents of messages that are exchanged by the devices in the payment card registration processing.

[1819] First, when the user performs an electronic payment card registration operation 6504, the mobile user terminal generates a payment card registration request 6505 and transmits it to the service providing system via digital wireless telephone communication.

[1820] As is shown in Fig. 107A, the digital signature of a user is provided for data that consists of a payment card registration request header 10700, which is header information indicating that the message is the payment card registration request 6505 and describing the data structure; a card ID 10701 of a payment card to be registered; a user ID 10702; and an issued time 10703, which indicates the date on which the payment card registration request 6505 was issued. These data are closed and addressed to the service provider, thereby providing the payment card registration request 6505.

[1821] The user processor of the service providing system decrypts the received payment card registration request 6505 and examines the digital signature, and transmits the request 6505 to the service manager processor. The service manager processor generates a service director processor to form a process group that processes a payment card registration request 10704. The service director processor ascertains that the electronic payment card indicated by the card ID 10701 is registered in the payment card list 4611 for the user in the user information server 902, and registers that electronic payment card in the registered card list 5402 for electronic payment cards of the service director information server 901. At this time, the service director processor newly generates a card signature private key and a card signature public key pair. Further, the service director processor generates a registered card certificate using the card signature public key, and registers it in the registered card list 5402. The service director processor then generates a card certificate issuing message 10713 using the card signature private key and the registered card certificate that has been generated. The user processor closes the card certificate issuing message 10713 and addresses it to the user, and transmits it as a payment card certificate issuing message 6506 to the mobile user terminal via digital wireless telephone communication.

[1822] As is shown in Fig. 107B, the digital signature of a service provider is provided for data that consists of a card certificate issuing header 10708, which is header information indicating that the message is the payment card certificate issuing message 6506 and describing the data structure; a card digital signature private key 10709; a registered card certificate 10710; a service provider ID 10711, and an issued time 10712, which indicates the date on which the payment card certificate issuing message 6506 was issued. These data are closed and addressed to the user, thereby providing the payment card certificate issuing message 6506.

[1823] The mobile user terminal 100 decrypts the received payment card certificate issuing message 6506 and examines the digital signature, replaces the card signature private key and the card certificate of an electronic payment card with the card signature private key 10709 and the registered card certificate 10710, both of which are included in the payment card certificate issuing message 6506, changes the registration state in the card status to the post-registration state, and displays on the LCD the electronic payment card that has been registered (display a payment card that is registered; 6507).

[1824] An explanation will now be given for the contents of messages that are exchanged by the service providing system 110 and the merchant terminal 102, the merchant terminal 103, or the accounting machine 3555 (automatic vending machine 104) during the payment card setup processing.

[1825] The payment card setup processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1826] Therefore, for the payment card setup process, the procedures for the exchange of messages by the service providing system and the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and the contents (data structures) of the messages to be exchanged are the same as those used for the above described data updating processing (Figs. 57 and 88).

[1827] It should be noted, however, that the payment card setup process is not performed each time the data updating process is performed, but when the payment card list 4609 for the merchant stored in the merchant information server 903 is updated by the service director processor.

[1828] When the payment card list 4609 is updated, the merchant processor includes updated data in the payment card list 4609 for the compressed update data 8828 in the update data 5705, and transmits the resultant data as update data 5705 to the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1829] Upon receiving the update data 5705, the merchant terminal 102 (the merchant terminal 103 or the accounting machine 3555) decompresses the update data 8828, and updates the data in the RAM and on the hard disk. At this time, the payment card list 2811 (3211 or 3608) in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) is updated, and an electronic payment card that is handled by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) is updated.

[1830] An explanation will now be given for the contents of messages that are exchanged by between the mobile ussr terminal 100 and the merchant terminal 102, the merchant terminal 103, or the accounting machine 3555 (automatic vending machine 104) during the payment card clearing processing.

[1831] In Fig. 68 are shown procedures for the exchange of messages by the mobile user terminal 100 and the merchant terminal 102 or 103 during the payment card clearing processing, and in Fig. 69 are shown procedures for the exchange of by the mobile user terminal 100 and the accounting machine 3555. In Figs. 112A and 112B and Figs. 113A and 113B are shown the contents of messages that are exchanged by the devices during the payment card clearing processing. For the payment card clearing processing, the same procedures are employed for the exchange of messages by the mobile user terminal 100 and the merchant terminal 102, the merchant terminal 103 or the accounting machine 3555, and the same contents (data structures) are included in the messages to be exchanged.

[1832] First, when a user performs a payment offer operation 6804 or 6906, the mobile user terminal employs a payment card that is to be used for payment and an arbitrarily generated test pattern and produces a payment offer message 6805 or 6907, which is a message for offering the merchant the payment of a price. The mobile user terminal transmits the message 6805 or 6907 to the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) via infrared communication.

[1833] As is shown in Fig. 112A, the payment offer message 6805 or 6907 consists of a payment offer header 11200, which is header information indicating that the message is the payment offer message 6805 or 6907 and describes the data structure; a service code 11201, which identifies the request for payment using an electronic payment card; a request number 11202, which is an arbitrarily generated number that uniquely represents the payment card clearing process; an amount of payment 11203 that is entered by the user; a presentation card 11203 for presenting an electronic payment card to be used for the payment; a

card certificate 11205; a current card status 11206 for an electronic payment card to be used for the payment; a total remaining value 11207; a card ID 11208; an issued time 11209, which indicates the date on which the payment offer message 6805 or 6907 was issued; and an accounting machine test pattern 11211, which is an arbitrarily generated test pattern. The digital signature is provided, using the card signature private key of an electronic payment card, for the card status 11206, the total remaining value 11207, the card ID 11208 and the issued time 11209. The accounting machine test pattern 11211 is encrypted using the accounting machine public key.

[1834] The presentation card 11204, the card certificate 11205, the card status 11206, the total remaining value 11207, the card ID 11208 and the issued date 11209 specify the contents of the electronic payment card for the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and the accounting machine test pattern 11211 is a test pattern for authorizing the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1835] Upon receiving the payment offer 6805 or 6907, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) refers to the payment card list 2811 (3211 or 3608) and activates a payment card clearing module that corresponds to the card code (included in a presentation card) for the electronic payment card that is presented. Then, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) examines the validity of the contents of the payment offer 6805 or 6907, generates a payment offer response 6806 or 6908, which is a response message for the payment offer, and transmits it to the mobile user terminal via infrared communication. When the electronic payment card that is presented is not registered in the payment card list 2811 (3211 or 3608), the payment offer response 6806 or 6907 is transmitted, which indicates that the pertinent electronic payment card is not available.

[1836] In the verification processing for determining the validity of the payment offer message 6805 or 6907, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) verifies that for the sale the amount of payment 11203 designated by the user is adequate. The merchant terminal 102 employs the fact that the card certificate 11205 is a registered card certificate, and examines the card status 11206 and the total remaining value 11207 to determine whether the electronic payment card is valid and can be used as a payment card for the payment. Then, the merchant terminal 102 examines the presentation card 11204, the digital signature of the service provider that is provided for the card certificate 11205, and the validity term. Further, the merchant terminal employs the card signature public key of the card certificate 11205 to examine the digital signature of the electronic payment card that is provided for the card status 11206, the total remaining value 11207, the card ID 11208 and the issued time 11209. In this fashion, the validity of the payment offer 6805 or 6907 is verified.

[1837] In the generation of the payment offer response 6806 or 6908, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) decrypts the accounting machine test pattern 11211 using the accounting machine private key, and employs the card public key to encrypt the card test pattern 11211 that is arbitrarily generated.

[1838] As is shown in Fig. 112B, the digital signature of a merchant is provided for the data that consists of a payment offer response header 11213, which is header information indicating that the message is the payment offer response 6806 or 6908 and describing the data structure; a transaction number 11214; a response message 11215; a request number 11216; a card ID 11217; an instruction code 11218; an amount of sales 11219, which indicates the price that is charged or the cost of the service that is calculated by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555); an accounting machine test pattern 11220, which is decrypted; a card test pattern 11221, which is an arbitrarily generated test pattern; an accounting machine ID 11223; a merchant ID 11224; and an issued time 11225, which indicates the date on which the payment offer response 6805 or 6908 was issued. In this fashion, the payment offer response 6806 or 6908 is provided. The card test pattern 11221 is encrypted using the card public key.

[1839] The transaction number 11214 is a number that is arbitrarily generated, by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and that uniquely represents the payment card clearing process. When, as a result of the examination of the payment offer 6805 or 6907, the payment card clearing process can not be performed (the amount of the payment entered by the user is not sufficient, or when an electronic payment card is one that can not be handled by the pertinent merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555)), a value of 0 is set. When the payment card clearing process can be performed, a value other than 0 is set.

[1840] The response message 11215 is text information constituting the message transmitted by the merchant to the user. When the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) can not handle an electronic payment card that has been presented (transaction number = 0), data to that effect is included in the response message. The response message is prepared optionally, and may not be prepared.

[1841] The instruction code 11218 is command code information for an electronic payment card, and is used when a value equivalent to the amount of sales 11219 is subtracted from the total remaining value held by the electronic payment card. The instruction code is varied by combining the electronic payment card transaction module and the payment card clearing module.

[1842] When the mobile user terminal receives the payment offer response 6806 or 6908, first, for verification of to verify the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), it compares the accounting machine test pattern 11211 with the accounting machine test pattern 11220 included in the payment offer response 6806 or 6908. The mobile user terminal ascertains whether the amount of sales 1219 is equal to or smaller than the amount of payment 11203 entered by the user, and subtracts the amount of sales 11219 from the total remaining value held by the electronic payment card in accordance with the instruction code 11218. Then, the mobile user terminal decrypts the card test patten using the card private key, and generates a micro-check message 6807 or 6909, which corresponds to a check that has as its face value the amount of the sale. The check is transmitted via infrared communication to the merchant terminal 102 (or to the merchant terminal 103 or the accounting machine 3555).

[1843] As is shown in Fig. 113A, the digital signature using the card signature private key and the digital signature of a user are provided for the data that consists of a micro-check header 11300, which is header information indicating that the message is the micro check 6807 or 6909 and describing the data structure; a micro-check issuing number 11301, which indicates the order of the payment card clearing process; a card test pattern 11302, which is decrypted; an amount of payment 11303, which indicates the obtained value that is subtracted from the total remaining value; a card status 11304; a total remaining value 11305 available after the subtraction; an accounting machine ID 11306; a merchant ID 11307; a request number 11308; a transaction number 11309; a card code 11310; a card ID 11311; and an issued time 11312, which indicates the date on which the micro-check 6807 or 6909 was issued. In this fashion, the micro-check 6807 or 6909 is provided.

[1844] Upon receiving the micro-check 6807 or 6909, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) authorizes the electronic payment card by comparing the card test pattern 11221 with the card test pattern 11302 that is included in the micro-check 6807 or 6909, examines the validity of the contents of the micro-check 6807 or 6909, and generates a receipt 6808 or 6910 and transmits it to the mobile user terminal via infrared communication.

[1845] In the verification process for the validity of the micro-check 6807 or 6909, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) determines whether the amount of payment 11303 represented by the micro-check 6807 or 6909 is adequate for the value of the sale. Also, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) determines whether the value obtained by subtracting the total remaining value 11305 from the total remaining value 11207, which represents the payment offer, is equal to the amount of payment 11303 represented by the micro-check. Finally, the merchant terminal 102 examines the digital signature of the electronic payment card accompanying the micro-check 6807 or 6909.

[1846] As is shown in Fig. 113B, the digital signature of a merchant is provided for the data that consists of a receipt header 11314, which is header information indicating that the message is the receipt 6808 or 6910 and describing the data structure; sales information 11315; a card ID 11316; a total receipt value 11317, which indicates the same value as the amount of payment 11303 represented by the micro-check that is received by the merchant; a request number 11318; a transaction number 11319; a micro-check issuing number 11320; an accounting machine ID 11321; a merchant ID 11322; and an issued time 11323, which indicates the date on which the receipt 6808 or 6910 was issued. In this fashion, the receipt 6808 or 6910 is provided.

[1847] The sales information 11315 is text information constituting the contents of a transaction acquired during the payment card clearing process, and corresponds to the specifications for the products that are

traded or for the service that is provided, or for a statement of account.

[1848] Upon receiving the receipt 6808 or 6910, the mobile user terminal verifies that the total receipt value 11317 is equal to the amount of payment 11303 of represented by the micro-check, and increments the micro-check issuing number. The mobile user terminal then registers the receipt 6808 or 6910 as usage information in the use list 1715, and displays the receipt 6808 or 6910 on the LCD (display the receipt; 6810 or 6911).

[1849] When the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) has transmitted the receipt 6808 or 6910, it registers, in the transaction list 2812 (3212 or 3609), the micro-check 6807 or 6909 and the receipt 6808 or 6910 as history information for the payment card clearing process.

[1850] The merchant terminal 102 or the merchant terminal 103 displays, on the LCD, a message that indicates the termination of the payment card clearing process (display the clearing completion; 6809), and the product is delivered by the merchant to the user (deliver the product; 6811). Thereafter, the accounting machine 3555 (automatic vending machine 104) discharges the product to the discharge port 703.

[1851] When the mobile user terminal receives the payment offer, and the amount of payment 11203 entered by the user is greater than the amount of sales 11219, the dialogue message for asking the user for the value of the payment is displayed on the LCD 303. When the user again enters a payment value that is greater than the amount of sales 11219, a micro-check having the entered value as the payment value 11303 may be issued. In this case, a value that corresponds to the difference between the amount of payment 11303 and the amount of sales 11219 can be paid as a commission to the merchant.

[1852] An explanation will now be given for the contents of messages that are exchanged by the devices during the payment card reference processing.

[1853] In Fig. 72 are shown procedures for the exchange of messages by the devices during the payment card reference processing, and in Figs. 88A to 88D and Fig. 116B are shown the contents of messages that are exchanged during the payment card reference processing. The payment card reference processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1854] Therefore, for the payment card reference process, the procedures for the exchange of messages by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) and the service providing system, and the contents (data structures) of the messages to be exchanged are the same as those employed for the above described data updating processing.

[1855] Compressed upload data 8818 in the upload data 5702 include a micro-check that is newly registered in the transaction list 2510 during the payment card clearing process conducted during the period extending from the previous performance of the data updating process to the current performance of the data updating process.

[1856] During the data updating processing, the merchant processor transmits, to the service manager processor, a message requesting the reference process be performed for the micro-check that is uploaded from the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555). The service manager processor generates a service director processor to form a process group for examining the validity of the micro-check.

[1857] First, the service director processor determines whether the accounting machine ID 11306 and the merchant ID 11307 in the micro-check match the accounting machine ID 5215 of the merchant and the merchant ID 5214. Then, the service director processor examines the registered card list 5402 in the service director information server 901 to verify that the electronic payment card for which the micro-check was issued is registered. The service director processor employs the user public key 5419 to examine the digital signature of the user that accompanies the micro-check, and employs the registered card certificate to examine the digital signature for the payment card that accompanies the micro-check. In addition, the service director processor employs the micro-check issuing number when examining the matching of the amount of payment with the total remaining value, and transmits the result of the examination to the merchant processor. As a result, the micro-check is registered in the micro-check list.

[1858] The merchant processor enters the received payment card reference results in the compressed update data 8828 in the update data 5705, and transmits the data 5705 to the merchant terminal 102 (or the merchant terminal 103).

[1859] When an error occurs in the process for verifying the validity of the micro-check, the service director processor transmits a message indicating that an error occurred in the management system 908.

[1860] Upon receiving the update data 5705, the merchant terminal 102 (or the merchant terminal 103) decompresses the update data 8828 and updates the data in the RAM and on the hard disk. At this time, the payment card reference results are registered in the authorization report list 2813 (3213) of the merchant terminal 102 (the merchant terminal 103).

[1861] If the firm represented by the merchant differs from that represented by the payment card issuer, and a payment for the merchant who handles the payment card is made by the payment card issuer, or if the usage of the payment card is periodically reported to the payment card issuer in accordance with the terms of a contract, in accordance with the micro-check that is newly registered in the micro-check list, the service director processor generates weekly, for example, a usage condition notification 11616, which is a message for notifying the payment card issuer of the payment card usage condition. The payment card issuer processor closes the notification 11616 and addresses it to the payment card issuer, and transmits it as a usage report 7200 to the payment card issuing system 108.

[1862] As is shown in Fig. 116B, the digital signature of a service provider is provided for the data that consists of a usage report header 11610, which is header information indicating that the message is the usage report 7200 and describing the data structure; a card ID and payment value list 11611 of payment cards that are employed; the merchant name 11612 and the merchant ID 11613 of a merchant that handles the payment card; a service provider ID 11614; and an issued time 11615, which indicates the date on which the usage report 7200 was issued. These data are closed and addressed to the payment card issuer, thereby providing the usage report 7200.

[1863] Upon receiving the usage report 7200, the payment card issuing system 108 decrypts it and examines the digital signature, and performs such processing as making a payment to the merchant.

[1864] An explanation will now be given for the contents of messages that are exchanged by the devices during the payment card transfer processing.

[1865] In Fig. 75 are shown procedures for the exchange of messages by the devices during the payment card transfer processing, and in Figs. 120A and 120B, 121A and 121B, and 122A and 122B are shown the contents of messages that are exchanged during the payment card transfer processing.

[1866] The payment card transfer process can be performed when the card status 2007 of the electronic payment card indicates the transfer enabled state, which is designated by the payment card issuer when issuing a payment card.

[1867] In Fig. 75 is shown a case where user A transfers an electronic payment card to user B. The procedures for the exchange of messages by the devices belonging to users A and B are the same for infrared communication as they are for digital wireless communication. The data structures of messages are also the same.

[1868] In Fig. 75, first, when user A performs a payment card transfer process 7500, the mobile user terminal of user A transmits a payment card transfer offer 7501, which is a message offering to transfer an electronic payment card, to the mobile user terminal of user B. When at this time the mobile user terminals of user A and user B are connected, communication between user A and user B is performed via digital wireless telephone. When the mobile user terminals are not connected, infrared communication is employed.

[1869] As is shown in Fig. 120A, the digital signature of user A is provided for the data consisting of a card transfer offer header 12000, which is header information indicating that the message is the card transfer offer 7501 and describing the data structure; a transfer offer number 12001, which is an arbitrarily generated number that uniquely represents the payment card transfer process; a presentation card 12002 and a card certificate 12003 for an electronic payment card to be transferred; a card status 12004; a total

remaining value 12005; a card ID 12006; an issued time 12007, which indicates the date on which the card transfer offer 7501 was issued; and a user public key certificate 12009. In this fashion, the card transfer offer 7501 is provided. The digital signature of the electronic payment card is provided, using the card signature private key, for the card status 12004, the variable card information 12005, the card ID 12006 and the issued time 12007.

[1870] The digital signature of the service provider is provided for the data that consist of a user public key header 12010; the user public key 12011 of user A; a public key certificate ID 12012, which is ID information for the public key certificate; a certificate validity term 12013; a service provider ID 12014; and a certificate issued time 12015. In this fashion, the user public key certificate 12009 is provided.

[1871] Upon receiving the card transfer offer 7501, the mobile user terminal of user B examines the presentation card 12002, the card certified 12003, and the digital signature of the service provider and the validity term of the public key certificate 12009. Then, the mobile user terminal examines the digital signature of the electronic payment card that is provided for the card status 12004, the total remaining value 12005, the card ID 12006 and the issued time 12007, and the digital signature of user A accompanying the card transfer offer 7501, and verifies the contents of the card transfer offer 7501. In accordance with the presentation card 12002, the card status 12004 and the total remaining value 12005, the mobile user terminal then displays, on the LCD, the contents of the electronic payment card that is to be transferred (display the transfer offer; 7502).

[1872] When user B performs a transfer offer acceptance operation 7503, the mobile user terminal of user B transmits, to the mobile user terminal of user A, a card transfer offer response 7504, which is a response message for the card transfer offer 7501.

[1873] As is shown in Fig. 120B, the digital signature of user B is provided for the data that consist of a card transfer offer response header 12016, which is header information indicating that the message is the card transfer offer response 7504 and describing the data structure; an acceptance number 12017; a transfer offer number 12018; a card ID 12019; an issued time 12020, which indicates the date on which the card transfer offer response 7504 was issued; and a user public key certificate 12021. In this fashion, the card transfer offer response 7504 is provided.

[1874] The user public key certificate 12021 is a public key certificate for user B. To provide this certificate 12021, the digital signature of the service provider is provided for the data that consist of a user public key certificate header 12022; a user public key 12023 for user B; a public key certificate ID 12024, which is ID information for the public key certificate; a certificate validity term 12025; a service provider ID 12026; and a certificate issued time 12027.

[1875] The acceptance number 12017 is arbitrarily generated, by the mobile user terminal of user B, as a number that uniquely represents the payment card transfer processing. With this number, the mobile user terminal of user A is notified as to whether user B has accepted the card transfer offer 7501. When user B does not accept the card transfer offer 7501, a value of 0 is set as the acceptance number 12017. When user B accepts the card transfer offer 7501, a value other than 0 is set.

[1876] Upon receiving the card transfer offer response 7504, the mobile user terminal of user A displays, on the LCD, the contents of the card transfer offer response 7504 (display the transfer offer response; 7505). When the card transfer offer 7501 is accepted (acceptance number 12017 NOTEQUAL 0), the mobile user terminal of user A examines the digital signature of the service provider of the user public key certificate 12021 and the validity term. The mobile user terminal generates a card transfer certificate 7506, which is a message that corresponds to a transfer certificate for an electronic payment card to user B, and transmits it to the mobile user terminal of user B.

[1877] As is shown in Fig. 121A, the digital signature of the electronic payment and the digital signature of user A are provided for the data that consist of a card transfer certificate header 12100, which is header information indicating that the message is the card transfer certificate 7506 and describing the data structure; a presentation card 12101 for an electronic payment card to be transferred; a card status 12102; a total remaining value 12103; a transfer offer number 12104; an acceptance number 12105; a public key certificate ID 12106 for the user public key certificate of user B; a public key certificate ID 12107 for the user public key certificate of user A; a card ID 12108; and an issued time 12109, which indicates the date on which the card transfer certificate 7506 was issued. These data are closed and addressed to user B, thereby providing the card transfer certificate 7506.

[1878] Upon receiving the card transfer certificate 7506, the mobile user terminal of user B decrypts it and examines the digital signature of user A and the one accompanying the electronic payment card. Further, the mobile user terminal compares the card ID presented by the card transfer offer 7501 with the card ID 12108, and compares the public key certificate IDs 12106 and 12107 with the public key certificates of users B and A to verify the contents of the card transfer certificate 7506. The mobile user terminal then generates a card transfer receipt 7507, which is a message indicating the electronic payment card has been received, and transmits the receipt 7507 to the mobile user terminal of user A.

[1879] As is shown in Fig. 121B, the digital signature of user B is provided for the data that consist of a card transfer receipt header 12115, which is header information indicating that the message is the card transfer receipt 7507 and describing the data structure; a card ID 12116; a transfer offer number 12117; an acceptance number 12118; a public key certificate ID 12119 for the user public key certificate of user A; a public key certificate ID 12120 for the user public key certificate of user B; and an issued time 12121, which indicates the date on which the card transfer receipt 7507 was issued. These data are closed and addressed to user A, thereby providing the card transfer receipt 7507.

[1880] Upon receiving the card transfer receipt 7507, the mobile user terminal of user A decrypts it, and examines the digital signature of user B. Further, the mobile user terminal compares the public key certificate IDs 12119 and 12120 with the public key certificates of users B and A to verify the contents of the card transfer receipt 7507. The mobile user terminal then erases the transferred electronic payment card from the card list 1713, and registers the card transfer receipt 12122 in use history 1715. At this time, addresses in the object data area at which the transfer offer number, the code information indicating the card transfer process, the issued time for the card transfer receipt 7507 and the card transfer receipt 12122 are stored are assigned to the request number 1840 in the use list 1715, the service code 1841, the use time 1842 and the use information address 1843.

[1881] The mobile user terminal of user A displays, on the LCD, a message indicating the completion of the transfer process (display the transfer process; 7508). The process at the mobile user terminal of user A (sender) is thereafter terminated.

[1882] After transmitting the card transfer receipt 7507, the mobile user terminal of user B displays the received card transfer certificate 12111 on the LCD. In addition, the mobile user terminal displays a dialogue message inquiring whether the transfer process with the service providing server (process for downloading the received electronic payment card from the service providing system) should be immediately performed (display the transfer certificate; 7509).

[1883] The dialogue message has two operating menus: "transfer process request" and "cancel." When "cancel" is selected, the transfer process performed with the service providing server is canceled, and in the process (data updating process) during which the service providing system updates the data in the mobile user terminal, an electronic payment card that has been transferred is assigned to the mobile user terminal.

[1884] When user B selects "transfer process request" (transfer process request operation; 7510), based on the card transfer certificate 12111 the mobile user terminal generates a card transfer request 7511, which is a message requesting that the transfer process be performed with the service providing system, and transmits it to the service providing system via digital wireless telephone communication.

[1885] As is shown in Fig. 122A, the digital signature of user B is provided for the data that consists of a card transfer request header 12200, which is header information indicating that the message is the card transfer request 7511 and describing the data structure; a decrypted card transfer certificate 12201 (12111); the user ID 12202 of user B; and an issued time 12203, which indicates the date when the card transfer request 7511 was issued. These data are closed and addressed to the service provider, thereby providing the card transfer request 7511.

[1886] Upon receiving the card transfer request 7511, the user processor of user B of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the card transfer request 12204.

[1887] The service director processor, first refers to the user list 5200 and specifies the recipient (user B)

and the sender (user A) of the transfer process by employing the public key certificate IDs 12106 and 12107 in the card transfer certificate 12201 that is included in the card transfer request 12204. The service director processor examines the digital signature of the user A and the digital signature accompanying the electronic payment card, which are provided for the card transfer certificate 12201, and verifies the validity of the card transfer certificate 12201. Following this, the service director processor erases the electronic payment card to be transferred from the card list 4611 of the user A that is stored in the user information server 902. Then, the service director processor changes the card signature private key and card signature public key pair and the card certificate for a new key pair and a card certificate, and also changes the card status and the total remaining value to the card status 12102 and to the total remaining value 12103 for the card transfer certificate 12201. The service director processor generates an electronic payment card received from user A, and enters it in the card list 4611 for the user B.

[1888] When the electronic payment card that is to be transferred has already been registered, the service director processor updates the registered card list 5402 holding the electronic payment card. Specifically, the user ID 5418, the user public key 5419, the registered card certificate address 5420, the micro-check list address 5421 and the former user information address 5422, all of which are in the registered card list 5402, are updated (to the information for user B). The old information (information for user A) is pointed to at the former user information address 5422 as former user information 5423..

[1889] The service director processor generates a payment card transfer message 12215, which includes an electronic payment card transferred from user A. The user processor of user B closes the message 12215 and addresses it to the user B, and transmits it as a payment card transfer message 7512 to the mobile user terminal of user B via digital wireless telephone communication.

[1890] As is shown in Fig. 122B, the digital signature of the service provider is provided for the data that consist of a payment card transfer header 12208, which is header information indicating that the message is the card transfer 7512 and describing the data structure; a transfer number 12209, which is an arbitrarily generated number that represents the transfer process in the service providing system; transfer information 12210; an acceptance number 12211; an electronic payment card 12212, which is transferred; a service provider ID 12213; and an issued time 12214, which indicates the date when the payment card transfer message 7512 was issued. These data are closed and addressed to the user B, thereby providing the card transfer message 7512.

[1891] The transfer information 12210 is information concerning the electronic payment card transfer process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1892] The mobile user terminal of user B decrypts the received payment card transfer message 7512 and examines the digital signature, registers the electronic payment card 12212 in the card list 1713, and displays the electronic payment card on the LCD (display the electronic payment card; 7513). The card transfer process is thereafter terminated.

[1893] An explanation will now be given for the contents of messages that are exchanged by the devices during the electronic payment card installation processing.

[1894] In Fig. 78 are shown procedures for the exchange of messages by the devices during the electronic payment card installation processing, and in Figs. 125A and 125B, and 125A and 125B are shown the contents of messages that are exchanged during the electronic payment installation processing.

[1895] First, when the user performs an electronic payment card installation operation 7800, the mobile user terminal generates an electronic payment card installation request 7801, and transmits it to the service providing system 110 via digital wireless telephone communication.

[1896] As is shown in Fig. 125A, the digital signature of the user is provided for the data that consists of an electronic payment card installation request header 12500, which is header information indicating that the message is the electronic payment card installation request 7801 and describes the data structure; an installation card number 12501 and an installation number 12502, which are entered by a user; a request number 12503, which is an arbitrarily generated number that uniquely represents the electronic payment card installation process; a user ID 12504; and an issued time 12505, which indicates the date when the electronic payment card installation request 7801 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card installation request 7801.

[1897] Upon receiving the electronic payment card installation request 7801, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the electronic payment card installation request 12506.

[1898] First, the service director processor refers to the installation card list that is indicated by the installation card list address 5236 for the payment card issuer list 5204, and specifies a payment card issuer who issues a payment card that is represented by the installation number 12501. The service director processor generates a payment card installation request 12517, which is a message requesting that the payment card issuer issue a payment card using the installation card. The payment card issuer processor closes the request 12517 and addresses it to the payment card issuer, and transmits it as a payment card installation request 7802 to the payment card issuing system 108.

[1899] As is shown in Fig. 125B, the digital signature of the service provider is provided for the data that consist of a payment card installation request header 12510, which is header information indicating that the message is the payment card installation request 7802 and describing the data structure; an installation card number 12511; an installation number 12512; a request number 12513; a customer number 12514, which uniquely represents a user for the payment card issuer; a service provider ID 12515; and an issued time 12516, which indicates the date when the payment card installation request 7802 was issued. These data are closed and addressed to the payment card issuer, thereby providing the payment card installation request 7802.

[1900] Upon receiving the payment card installation request 7802, the payment card issuing system 108 decrypts it and examines the digital signature. The payment card issuing server 1200 compares the installation card number 12511 and the installation number 12512, which are included in the payment card installation request 7802, with the management information for the issued electronic payment card installation card that is stored in the payment card issuing information server 1202. The payment card issuing server 1200 then updates the data in the customer information server 1202 and the payment card issuing information server 1203. Furthermore, the payment card issuing server generates payment card data (12606) for a requested payment card, and transmits, to the service providing system, an electronic payment card installation commission 7803, which is a message requesting the installation of an electronic payment card that corresponds to the requested payment card.

[1901] As is shown in Fig. 126A, the digital signature of the payment card issuer is provided for the data that consists of an electronic payment card installation commission header 12600, which is header information indicating that the message is the electronic payment card installation commission 7803 and describing the data structure; a transaction number 12601, which is an arbitrarily generated number that uniquely represents the transaction with a user; payment card issuing information 12602; a request number 12603; card code 12604, which indicates the type of electronic payment card that is to be issued; a template code 12605, which indicates a template program for an electronic payment card to be issued; payment card data 12606; representative component information 12607; a payment card issuer ID 12608; and an issued time 12609, which indicates the date when the electronic payment card installation commission 7803 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card installation commission 7803.

[1902] The payment card issuing information 12602 is information concerning the payment card issuing process performed by the payment card issuing system, and is accompanied by the digital signature of the payment card issuer.

[1903] The payment card data 12606 is payment card information issued by the payment card issuer, wherein the digital signature of the payment card issuer accompanies the data that consists of the card ID 12614, the payment card information 12615 and the card ID 12616.

[1904] The payment card issuer processor of the service providing system decrypts the received electronic payment card installation commission 7803 and examines the digital signature, and transmits the commission 7803 to the service director processor. In accordance with the electronic payment card installation commission 12610, the service director processor generates an electronic payment card to be issued to a user, using the same procedures as are used for the payment card purchase processing, and also generates an electronic payment card installation message 12615, which is a message directing that the electronic payment card be installed in the mobile user terminal. The user processor closes the

electronic payment card installation message 12655 and addressees it to a user, and transmits it as an electronic payment card installation message 7804 to the mobile user terminal via digital wireless telephone communication.

[1905] As is shown in Fig. 126B, the digital signature of the service provider is provided for the data that consists of an electronic payment card installation header 12617, which is header information indicating that the message is the electronic payment card installation message 7804 and describing the data structure; a transaction number 12618; payment card issuing information 12619, which concerns the payment card issuing process performed by the payment card issuing system; payment card issuing information 12620, which concerns the payment card issuing process performed by the service providing system; a request number 12621; generated electronic payment card data 12622; a service provider ID 12623; and an issued time 12624, which indicates the date when the electronic payment card installation message 7804 was issued. These data are closed and addressed to the user, thereby providing the electronic payment card installation message 7804. The payment card issuing information 12619 and the payment card issuing information 12620 are accompanied by the digital signatures of the payment card issuer and the service provider.

[1906] The mobile user terminal decrypts the received electronic payment card installation message 7804 and examines the digital signature, registers, in the card list 1713, the electronic payment card included in the electronic payment card installation request 7804, and displays the installed electronic payment card on the LCD (display the electronic payment card; 7805).

[1907] An explanation will now be given for the contents of messages that are exchanged by devices in various processes for electronic telephone card service.

[1908] First, an explanation will be given for the contents of messages that are exchanged by devices during the telephone card purchase processing.

[1909] In Fig. 63 are shown the procedures for the exchange of messages by devices during the telephone card purchase processing. In Figs. 101A and 101B, 102A and 102B, 103A and 103B, 104A and 104B, and 105A and 105B are shown the contents of messages that are exchanged by devices during the telephone card purchase processing.

[1910] First, when a user performs a telephone card purchase order operation 6300, the mobile user terminal transmits a telephone card purchase order 6301 to the service providing system through digital wireless telephone communication.

[1911] As is shown in Fig. 101A, the digital signature of a user is provided for data that consists of a telephone card purchase order header 10100, which is header information identifying the message as the telephone card purchase order 6301 and describing the data structure; a response code 10101, which identifies the type of service requested by the user; a card order code 10102, which identifies an order code for a telephone card that is entered by the user; a number of telephone cards 10103 that the user has entered; a payment service code 10104, which identifies a credit card designated by the user; a payment value 10105; a payment option code 10106, which identifies a payment option, such as the number of payments designated by the user; a request number 10107, which is an arbitrarily generated number that uniquely represents the telephone card purchase processing; a validity term 10108 for the telephone card purchase order 6301; a user ID 10109; and an issued time 10110, which is the date on which the telephone card purchase order 6301 was issued. These data are closed and addressed to the service provider, thereby providing the telephone card purchase order 63@01. The service code 8901 identifies the purchase order of a telephone card to a telephone card issuer who is selected by the user.

[1912] Upon receiving the telephone card purchase order 6301, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group that processes a telephone card order 10111. The service director processor refers to the telephone card issuer list 5205 and generates a telephone card purchase order 10126 for the telephone card issuer indicated by the service code 10101. The telephone card issuer processor closes the telephone card order and addresses it to the telephone card issuer, and transmits the resultant order as a telephone card purchase order 6302 to the telephone card issuing system 109.

[1913] As is shown in Fig. 101B, the digital signature of a service providing system is provided for data that

consists of a telephone card purchase order header 10115, which is header information indicating that the message is the telephone card purchase order 6302 and describing the data structure; a card order code 10116; a number of cards 10117 that are purchased; a payment service code 10118; a payment value 10119; a payment option code 10120; a request number 10121; a customer number 10122, which uniquely represents a user for the telephone card issuer; a validity term 10123 for the telephone card purchase order 6302; a service provider ID 10124; and an issued time 10125, which is the date on which the telephone card purchase order 6302 was issued. These data are closed and addressed to the telephone card issuer, thereby providing the telephone card purchase order 6302.

[1914] When there was a previous transaction to which the user and the telephone card issuer were parties, a customer number that is registered in the customer table of the telephone card issuer is established as the customer number 10122. When there was no previous transaction, the service director processor generates for the telephone card issuer a number that uniquely represents the user, establishes it as the customer number 10122, and registers that number in the customer table. The customer table is designated by using the customer table address 5244 of the telephone card issuer list 5205.

[1915] Upon receiving the telephone card purchase order 6302, the telephone card issuing system 109 decrypts it and examines the digital signature. The telephone card issuing server 1300 updates the data in the customer information server 1301, the telephone card issuing information server 1302 and the telephone card information server 1303, generates telephone card data (10219) for the ordered telephone card, and transmits, to the service providing system, an electronic telephone card issuing commission 6303, which constitutes a message requesting the process for issuing an electronic telephone card that corresponds to the telephone card and the process for settling the price of the telephone card.

[1916] As is shown in Fig. 102A, the digital signature of a telephone card issuer is provided for data that consists of an electronic telephone card issuing commission header 10200, which is header information identifying the message as the electronic telephone card issuing commission 6303 and describing the data structure; a transaction number 10201, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 10202, which conveys the price of a telephone card; a clearing option 10203, which indicates which clearing procedures apply; a request number 10204; a telephone card code 10205, which identifies the type of electronic telephone card that is to be issued; a template code 10206, which identifies a template program to be used for an electronic telephone card that is to be issued; a number of telephone cards 10207, which indicates how many telephone cards are to be issued; telephone card data 10208; representative component information 10209; a telephone card issuer ID 10210; and an issued time 10211, which is the date on which the electronic telephone card issuing commission 6303 was issued. These data are closed and addressed to the service provider, thereby providing the electronic telephone card issuing commission 6303.

[1917] The clearing option 10203 is information by which the telephone card issuing system designates, to the service providing system, the procedures to be used for clearing the price of a telephone card. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic telephone card to a user after the price of the telephone card has been cleared, and a delayed clearing process for clearing the price of a telephone card after an electronic telephone card has been issued. The clearing option 10203 is used to designate either clearing process.

[1918] In the delayed clearing process, since an electronic telephone card is issued to a user before the clearing process is performed, the user does not have to wait.

[1919] For example, based on a purchase history maintained for customers, the telephone card issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known to be trustworthy, and can designate the spontaneous clearing for a customer with whom it has had no previous dealings.

[1920] The telephone card data 10208 is telephone card information issued by the telephone card issuer. A number of telephone card information items equivalent to the number of telephone cards 10207 are established as the telephone card data 10208. For one telephone card, the digital signature of a telephone card issuer is provided for data that consist of a card ID 10216, card information 10217 and a telephone card issuer ID 10218, and the telephone card information is thereby provided. The telephone card information 10217 is ASCII information describing the contents of a telephone card. For the telephone card information 10217, the title of a telephone card, the face value of the telephone card that is issued, the usage condition, an issuer, and whether it can be transferred, are described using a form whereby tag

information representing information types is additionally provided.

[1921] The representative component information 10209 is information that is established as the representative component information 2132 for an electronic telephone card to be generated. Therefore, the representative component information 10209 may not be set for use.

[1922] The telephone card issuer processor of the service providing system receives the electronic telephone card issuing commission 6303, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic telephone card issuing process and the telephone card price clearing process in accordance with the clearing procedures designated by using the clearing option 10203.

[1923] In Fig. 63 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1924] For the spontaneous clearing, the service director processor generates a clearing request 10324, which is a message requesting the clearing of the price of a telephone card. The transaction processor processor closes the clearing request 10324 and addresses it to the transaction processor, and then transmits it as a clearing request 6304 to the transaction processing system 106.

[1925] As is shown in Fig. 103B, the digital signature of a service provider is provided for data that consists of a clearing request header 10314, which is header information indicating that the message is the clearing request 6304 and describing the data structure; a user clearing account 10315, which includes a credit card that corresponds to the payment service code designated by the user; a telephone card issuer clearing account 10316, which designates the clearing account of a telephone card issuer; a payment value 10317; a payment option code 10318; a request number 10319, which is issued by the mobile user terminal 100; a transaction number 10320, which is issued by the telephone card issuing system; a validity term 10321, which presents the period during which the clearing request 6304 is effective; a service provider ID 10322; and an issued time 10323, which indicates the date on which the clearing request 6304 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 6304.

[1926] The transaction processing system 106 receives the clearing request 6304, decrypts it and examines the digital Signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 6305, and transmits it to the service providing system 110.

[1927] As is shown in Fig. 104A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 10400, which is header information indicating that the message is the clearing completion notification 6305 and describing the data structure; a clearing number 10401, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 10402; a telephone card issuer clearing account 10403; a payment value 10404; a payment option code 10405; a request number 10406; a transaction number 10407; clearing information 10408 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 10409 for a telephone card issuer that is accompanied by the digital signature of the transaction processor; clearing information 10410 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 10411; and an issued time 10412, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 6305.

[1928] Upon receiving the clearing completion notification 6305, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 10413 to the service director processor. Upon receiving the clearing completion notification 10413, the service director processor generates a clearing completion notification 10430 for the telephone card issuer. The telephone card issuer processor closes the clearing completion notification 10430, and transmits it to the telephone card issuing system 109 as a clearing completion notification 6306 for the telephone card issuer.

[1929] As is shown in Fig. 104B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 10417, which is header information indicating that the message is the clearing completion notification 6306 and describing the data structure; a clearing number 10418; a customer number 10419; a telephone card issuer ID 10420; a payment service code 10421; a payment

value 10422; a payment option code 10423; a request number 10424; a transaction number 10425; clearing information 10426 for a telephone card issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 10427; a service provider ID 10428; and an issued time 10429, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the telephone card issuer, thereby providing the clearing completion notification 6306.

[1930] Upon receiving the clearing completion notification 6306, the telephone card issuing system decrypts it and examines the digital signature, and generates a receipt 6307 and transmits it to the service providing system.

[1931] As is shown in Fig. 105A, the digital signature of a telephone card issuer is provided for data that consists of a receipt header 10500, which is header information indicating that the message is the receipt 6307 and describing the data structure; a customer number 10501; telephone card issuing information 10502; a payment service code 10503; a payment value 10504; a payment option code 10505; a request number 10506; a transaction number 10507; clearing information 10508; a transaction processor ID 10509; a telephone card issuer ID 10510; and an issued time 10511, which indicates the date on which the receipt 6307 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 6307. The telephone card issuing information 10502 is information concerning the telephone card issuing process performed by the telephone card issuing system, and is accompanied by the digital signature of the telephone card issuer.

[1932] Upon receiving the receipt 6307, the telephone card issuer processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 10512 to the service director processor. The service director processor employs the receipt 10512 to generate a receipt 10523 for a user.

[1933] In addition, the service director processor generates a clearing completion notification 10430 for the telephone card issuing system, generates an electronic telephone card to be issued to the user, and further generates an electronic telephone card issuing message 10227 that includes the electronic telephone card that is generated.

[1934] The user processor closes the electronic telephone card issuing message 10227 and the receipt 10523 while addressing them to the user, and transmits them as an electronic telephone card issuing message 6308 and a receipt 6309 to the mobile user terminal 100 via digital wireless communication.

[1935] As is shown in Fig. 102B, the digital signature of a service provider is provided for data that consist of an electronic telephone card issuing header 10220, which is header information indicating that the message is the electronic telephone card issuing message 6308 and describing the data structure; a transaction number 10221; a request number 10222; the number of telephone cards 10223; electronic telephone card data 10224 that are generated; a service provider ID 10225; and an issued time 10226, which indicates the date on which the electronic telephone card issuing message 6308 was issued. These data are closed and addressed to the user, thereby providing the electronic telephone card issuing message 6308. The electronic telephone card data 10224 includes electronic telephone cards 10231 equivalent in number to the number of telephone cards 10223.

[1936] As is shown in Fig. 105B, the digital signature of a service provider is provided for data that consists of a receipt header 10516, which is header information indicating that the message is the receipt 6309 and describing the data structure; a user ID 10517; a receipt 10518 (10512) obtained by decryption; clearing information 10519 for a user that is accompanied by the digital signature of a transaction processor; telephone card issuing information 10520; a service provider ID 10521; and an issued time 10522, which indicates the date on which the receipt 6309 was issued. These data are closed and addressed to the user, thereby providing the receipt 6309. The telephone card issuing information 10520 is information for the electronic telephone card issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1937] Upon receiving the electronic telephone card issuing message 6308 and the receipt 6309, the mobile user terminal decrypts them and examines the digital signatures, enters in the telephone card list 1714 an electronic telephone card included in the electronic telephone card issuing message 6308, enters the receipt 10523 in the use list 1715, and displays the electronic telephone card on the LCD 303.